- Mindy Higgins Bero (Hickok & Boardman) – insurance representative
- Jennifer Vander Veer (FBI) –federal investigator/law enforcement
- Ryan Kriger (VT AGO) – state investigator/law enforcement

(Please let us know if the descriptions of your role meet your approval, or offer a suggestion if you would prefers something else; this is all flexible.)

It's time to start planning the scenario. Our idea is that it should involve a mid-sized business (<50 employees), and the scenario should involve spear-phishing and ransomware, as well as a reportable data breach. There should be something in the scenario for everyone to react to, and while our goal is to show best practices, it shouldn't run smoothly. There should be some curveballs.

Please help us with the following:

- If you have ideas for the scenario, email me, Sarah Anders, and Lauren Jandl (cc'd here) – no need to send them to everyone. We'll compile them into one email for consideration.
- Fill out the Doodle Poll (https://doodle.com/poll/v6nwxi4hs97e8h7g) with times that you're available for a call to flesh out these and other details.

Thanks again, we are looking forward to this exciting event!

-Ryan

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

Kriger, Ryan

From: Kriger, Ryan
Sent: Thursday, September 27, 2018 4:56 PM
To: Jerry Tarrant; Roszkowski, Heather; Matt Borick; Jonathan Rajewski; Sherman, Nick; MacLean, Alex; Jennifer A. Vander Veer; mbero@hbinsurance.com
Cc: Curtis, Christopher; Jandl, Lauren; Anders, Sarah; Clark, Charity; Donovan, Thomas
Subject: RE: Tech Jam Planning
Attachments: Tech Jam Panel Scenario.docx

Thank you all for helping to develop a scenario for the upcoming Tech Jam. Attached is a loose outline of the scenario. I think I left a lot of opportunities for each of you to provide useful information to the audience. Nothing is set in stone (Including the name of the company) and I think this could use more work, but I would welcome your input. Feel free to email me directly with ideas or send in a markup. We'll have another call in the next week or two, and then I think we should be ready for the Tech Jam.

-Ryan

From: Kriger, Ryan
Sent: Monday, September 17, 2018 11:14 AM
To: Jerry Tarrant <jtarrant@mywebgrocer.com>; Roszkowski, Heather <Heather.Roszkowski@uvmhealth.org>; Matt Borick <mborick@drm.com>; Jonathan Rajewski <rajewski@champlain.edu>; Sherman, Nick <nick@leoninepublicaffairs.com>; MacLean, Alex <alex@leoninepublicaffairs.com>; Jennifer A. Vander Veer <jennifer.vanderveer@ic.fbi.gov>; mbero@hbinsurance.com
Cc: Curtis, Christopher <Christopher.Curtis@vermont.gov>; Jandl, Lauren <Lauren.Jandl@vermont.gov>; Anders, Sarah <Sarah.Anders@partner.vermont.gov>; Clark, Charity <Charity.Clark@vermont.gov>; Donovan, Thomas <Thomas.Donovan@vermont.gov>
Subject: Tech Jam Planning

Dear All,

Thank you for joining us at Tech Jam on October 19! The exact time of the panel is TBD but we will alert you as soon as possible when the time is set. Please hold your calendars open for that date until we have a final time for presentation.

Here is the full list of participants:

- Attorney General T.J. Donovan or Public Protection Chief Chris Curtis – moderator
- Jerry Tarrant (MyWebGrocer) – business Leader
- Heather Roszkowski (UVMHN) – IT manager
- Matt Borick (Downs Rachlin) – legal advisor
- Jonathan Rajewski (Leahy Ctr @ Champlain) – forensics consultant
- Nick Sherman and/or Alexandra MacLean (Leonine Public Affairs) – public affairs/crisis communications
- Mindy Higgins Bero (Hickok & Boardman) – insurance representative
- Jennifer Vander Veer (FBI) –federal investigator/law enforcement

- Ryan Kriger (VT AGO) – state investigator/law enforcement

(Please let us know if the descriptions of your role meet your approval, or offer a suggestion if you would prefers something else; this is all flexible.)

It's time to start planning the scenario. Our idea is that it should involve a mid-sized business (<50 employees), and the scenario should involve spear-phishing and ransomware, as well as a reportable data breach. There should be something in the scenario for everyone to react to, and while our goal is to show best practices, it shouldn't run smoothly. There should be some curveballs.

Please help us with the following:

- If you have ideas for the scenario, email me, Sarah Anders, and Lauren Jandl (cc'd here) – no need to send them to everyone. We'll compile them into one email for consideration.
- Fill out the Doodle Poll (https://doodle.com/poll/v6nwxi4hs97e8h7g) with times that you're available for a call to flesh out these and other details.

Thanks again, we are looking forward to this exciting event!

-Ryan

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

Kriger, Ryan

From: Charles Storrow <chuck@leoninepublicaffairs.com>
Sent: Thursday, September 20, 2018 1:23 PM
To: Clark, Charity; Curtis, Christopher; Kriger, Ryan
Subject: Data Privacy

Dear Charity, Chris and Ryan,

FYI, FWIW, I am told that the US Chamber of Commerce has developed a set of principles for a federal data privacy regulatory scheme, and that there is actually a chance that Congress might address the issue.

See:

https://www.uschamber.com/issue-brief/us-chamber-privacy-principles

https://www.commerce.senate.gov/public/index.cfm/pressreleases?ID=240B5C17-CBD5-4039-A9E4-CF2FADFF4712

I'll see you next Tuesday.

Best—Chuck

Charles Storrow, Partner
Leonine Public Affairs, LLP
1 Blanchard Court, Suite 101
Montpelier, VT 05602
Cell: (802) 371-7863 – Direct Office: 802-552-4470

chuck@leoninepublicaffairs.com
http://www.leoninepublicaffairs.com/

Kriger, Ryan

From: Kriger, Ryan
Sent: Monday, September 17, 2018 11:14 AM
To: Jerry Tarrant; Roszkowski, Heather; Matt Borick; Jonathan Rajewski; Sherman, Nick; MacLean, Alex; Jennifer A. Vander Veer; mbero@hbinsurance.com
Cc: Curtis, Christopher; Jandl, Lauren; Anders, Sarah; Clark, Charity; Donovan, Thomas
Subject: Tech Jam Planning

Dear All,

Thank you for joining us at Tech Jam on October 19! The exact time of the panel is TBD but we will alert you as soon as possible when the time is set. Please hold your calendars open for that date until we have a final time for presentation.

Here is the full list of participants:

- Attorney General T.J. Donovan or Public Protection Chief Chris Curtis – moderator
- Jerry Tarrant (MyWebGrocer) – business Leader
- Heather Roszkowski (UVMHN) – IT manager
- Matt Borick (Downs Rachlin) – legal advisor
- Jonathan Rajewski (Leahy Ctr @ Champlain) – forensics consultant
- Nick Sherman and/or Alexandra MacLean (Leonine Public Affairs) – public affairs/crisis communications
- Mindy Higgins Bero (Hickok & Boardman) – insurance representative
- Jennifer Vander Veer (FBI) –federal investigator/law enforcement
- Ryan Kriger (VT AGO) – state investigator/law enforcement

(Please let us know if the descriptions of your role meet your approval, or offer a suggestion if you would prefers something else; this is all flexible.)

It's time to start planning the scenario. Our idea is that it should involve a mid-sized business (<50 employees), and the scenario should involve spear-phishing and ransomware, as well as a reportable data breach. There should be something in the scenario for everyone to react to, and while our goal is to show best practices, it shouldn't run smoothly. There should be some curveballs.

Please help us with the following:

- If you have ideas for the scenario, email me, Sarah Anders, and Lauren Jandl (cc'd here) – no need to send them to everyone. We'll compile them into one email for consideration.
- Fill out the Doodle Poll (https://doodle.com/poll/v6nwxi4hs97e8h7g) with times that you're available for a call to flesh out these and other details.

Thanks again, we are looking forward to this exciting event!

-Ryan

Ryan G. Kriger

Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

Kriger, Ryan

From: Charles Storrow <chuck@leoninepublicaffairs.com>
Sent: Tuesday, July 31, 2018 11:03 AM
To: Kriger, Ryan
Cc: Cornell-Brown, Rowan
Subject: RE: ANNOUNCEMENT First Hearing on Protecting the Privacy of Vermonters

Ryan,

Thanks for the email and thanks for scheduling another meeting.

We represent several ISPs and as you can imagine they are interested in the issue of whether the FCC's 2016 Privacy Order should be adopted in Vermont. However, while I will be at the meeting on August 6 I will not be in a position to speak to that issue at that time. However, it is likely our clients will provide input, either in writing or verbally at the 9/25 meeting, either directly or via a trade association.

Thanks, and I will see you on Monday.

Sincerely—Chuck Storrow

Charles Storrow, Partner
Leonine Public Affairs, LLP
1 Blanchard Court, Suite 101
Montpelier, VT 05602
Cell: (802) 371-7863 – Direct Office: 802-552-4470

chuck@leoninepublicaffairs.com
http://www.leoninepublicaffairs.com/

LEONINE
PUBLIC AFFAIRS

From: Kriger, Ryan <ryan.kriger@vermont.gov>
Sent: Tuesday, July 31, 2018 10:29 AM
To: Kriger, Ryan <ryan.kriger@vermont.gov>
Cc: Cornell-Brown, Rowan <rowan.cornell-brown@vermont.gov>; Curtis, Christopher <Christopher.Curtis@vermont.gov>; Clark, Charity <Charity.Clark@vermont.gov>; Diamond, Joshua <Joshua.Diamond@vermont.gov>
Subject: ANNOUNCEMENT First Hearing on Protecting the Privacy of Vermonters

All,

We hope to see from you or hear from you at the First Hearing on Protecting the Privacy of Vermonters, taking place **Monday, August 6, 9 am to 12 pm EST**, at 29 Church Street, 3rd Floor in Burlington, Vermont (best entrance for the public is located at 110 Cherry Street). The hearing will be moderated by Vermont Attorney General TJ Donovan.

If you wish to reserve time to speak or to submit written comments, please email rowan.cornell-brown@vermont.gov. The amount of time allocated will be based on the number of people who wish to speak. Time will be reserved at the end for additional speakers or discussion.

A follow-up meeting to be held on **Tuesday, September 25, 1 to 4 pm EST**, location TBD. If you have any questions or wish to speak one-on-one, please contact ryan.kriger@vermont.gov.

The dial-in number for this event will be:

[redacted]

As a reminder, the topics of discussion include:

- Adoption of regulations concerning telecommunications privacy and whether to model such rules after the FCC's 2016 Privacy Order, WC Docket No. 16-106, FCC 16-148, adopted Oct. 27, 2016. The request for this recommendation was made in Act 66 of 2017.
- Whether Vermont should designate a Chief Privacy Officer, and what the responsibilities of that Officer would be. This request was made in Act 171 of 2018.
- Whether to regulate businesses that handle the data of consumers with whom they have a direct relationship, as requested in Act 171.
- Questions, concerns, and recommendations regarding the implementation of the Data Broker Registry, as authorized in Act 171.
- Additional approaches to protecting the privacy and data security of Vermonters.

Sincerely,

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

Kriger, Ryan

From: Kriger, Ryan
Sent: Thursday, July 5, 2018 9:18 AM
To: Charles Storrow
Subject: RE: First Hearing on Protecting the Privacy of Vermonters

Correct, it's on Monday, August 6, as per the Press Release.

From: Charles Storrow <chuck@leoninepublicaffairs.com>
Sent: Thursday, July 5, 2018 8:46 AM
To: Kriger, Ryan <ryan.kriger@vermont.gov>
Subject: RE: First Hearing on Protecting the Privacy of Vermonters

Ryan,
August 8 is a Wednesday, and in a separate email Chris indicated the hearing had been rescheduled to the 6th. Am I correct in assuming the hearing is on Monday, August 6?
Thanks—Chuck Storrow

Charles Storrow, Partner
Leonine Public Affairs, LLP
1 Blanchard Court, Suite 101
Montpelier, VT 05602
Cell: (802) 371-7863 – Direct Office: 802-552-4470
chuck@leoninepublicaffairs.com
http://www.leoninepublicaffairs.com/

LEONINE PUBLIC AFFAIRS

From: Kriger, Ryan <ryan.kriger@vermont.gov>
Sent: Friday, June 29, 2018 12:34 PM
To: Kriger, Ryan <ryan.kriger@vermont.gov>
Cc: Curtis, Christopher <Christopher.Curtis@vermont.gov>
Subject: RE: First Hearing on Protecting the Privacy of Vermonters

I spoke too soon – the Office of has decided to push back the first hearing date in order to give people more time to prepare. The new date is **Monday, August 8, 9 am to 12 pm EST**, same location.
Please feel free to contact me with any questions or concerns.
-Ryan

From: Kriger, Ryan
Subject: First Hearing on Protecting the Privacy of Vermonters

I am writing to inform you of the first of a series of hearings to consider recommendations for legislative proposals to protect the privacy of Vermonters. You are receiving this email because your input into this discussion would be very valuable, and we seek to hear from a wide spectrum of voices in considering how best to proceed in this area. As you may know, Vermont takes the privacy and protection of its citizens very seriously and we seek to strike a balance between the need to protect our consumers and the needs of the business community to continue to develop a robust economy.
The hearing will take place on Thursday, July 12, from 1:00 - 4:00 pm at 29 Church Street, 3rd Floor in Burlington, Vermont (best entrance for the public is located at 110 Cherry Street). If you have any questions or concerns ahead of time, please feel free to email me or call me at 802-828-3170.
Topics under consideration will include, but not be limited to:

- Adoption of regulations concerning telecommunications privacy and whether to model such rules after the FCC's 2016 Privacy Order, WC Docket No. 16-106, FCC 16-148, adopted Oct. 27, 2016. The request for this recommendation was made in Act 66 of 2017.
- Whether Vermont should designate a Chief Privacy Officer, and what the responsibilities of that Officer would be. This request was made in Act 171 of 2018.
- Whether to regulate businesses that handle the data of consumers with whom they have a direct relationship, as requested in Act 171.
- Questions, concerns, and recommendations regarding the implementation of the Data Broker Registry, as authorized in Act 171.
- Changes that should be made to Vermont's Security Breach Notice Act, 9 V.S.A. § 2453.
- Questions or concerns regarding the State of Vermont's handling of citizen's data.
- Laws and regulations that can be adopted to encourage the growth of privacy-oriented technology companies in Vermont.
- The necessity of any additional approaches to protecting the data security and privacy of Vermont consumers.

If you do not want to receive further emails or know of others who should be on this list, please reply or email ago.datasecurity@vermont.gov.

Thank you,

Ryan

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

Kriger, Ryan

From: Charles Storrow <chuck@leoninepublicaffairs.com>
Sent: Thursday, July 5, 2018 8:46 AM
To: Kriger, Ryan
Subject: RE: First Hearing on Protecting the Privacy of Vermonters

Ryan,

August 8 is a Wednesday, and in a separate email Chris indicated the hearing had been rescheduled to the 6th. Am I correct in assuming the hearing is on Monday, August 6?

Thanks—Chuck Storrow

Charles Storrow, Partner
Leonine Public Affairs, LLP
1 Blanchard Court, Suite 101
Montpelier, VT 05602
Cell: (802) 371-7863 – Direct Office: 802-552-4470

chuck@leoninepublicaffairs.com
http://www.leoninepublicaffairs.com/

LEONINE
PUBLIC AFFAIRS

From: Kriger, Ryan <ryan.kriger@vermont.gov>
Sent: Friday, June 29, 2018 12:34 PM
To: Kriger, Ryan <ryan.kriger@vermont.gov>
Cc: Curtis, Christopher <Christopher.Curtis@vermont.gov>
Subject: RE: First Hearing on Protecting the Privacy of Vermonters

I spoke too soon – the Office of has decided to push back the first hearing date in order to give people more time to prepare. The new date is **Monday, August 8, 9 am to 12 pm EST**, same location.

Please feel free to contact me with any questions or concerns.

-Ryan

From: Kriger, Ryan
Subject: First Hearing on Protecting the Privacy of Vermonters

I am writing to inform you of the first of a series of hearings to consider recommendations for legislative proposals to protect the privacy of Vermonters. You are receiving this email because your input into this discussion would be very valuable, and we seek to hear from a wide spectrum of voices in considering how best to proceed in this area. As you

may know, Vermont takes the privacy and protection of its citizens very seriously and we seek to strike a balance between the need to protect our consumers and the needs of the business community to continue to develop a robust economy.

The hearing will take place on Thursday, July 12, from 1:00 - 4:00 pm at 29 Church Street, 3rd Floor in Burlington, Vermont (best entrance for the public is located at 110 Cherry Street). If you have any questions or concerns ahead of time, please feel free to email me or call me at 802-828-3170.

Topics under consideration will include, but not be limited to:

- Adoption of regulations concerning telecommunications privacy and whether to model such rules after the FCC's 2016 Privacy Order, WC Docket No. 16-106, FCC 16-148, adopted Oct. 27, 2016. The request for this recommendation was made in Act 66 of 2017.
- Whether Vermont should designate a Chief Privacy Officer, and what the responsibilities of that Officer would be. This request was made in Act 171 of 2018.
- Whether to regulate businesses that handle the data of consumers with whom they have a direct relationship, as requested in Act 171.
- Questions, concerns, and recommendations regarding the implementation of the Data Broker Registry, as authorized in Act 171.
- Changes that should be made to Vermont's Security Breach Notice Act, 9 V.S.A. § 2453.
- Questions or concerns regarding the State of Vermont's handling of citizen's data.
- Laws and regulations that can be adopted to encourage the growth of privacy-oriented technology companies in Vermont.
- The necessity of any additional approaches to protecting the data security and privacy of Vermont consumers.

If you do not want to receive further emails or know of others who should be on this list, please reply or email ago.datasecurity@vermont.gov.

Thank you,

Ryan

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

Kriger, Ryan

From: Charles Storrow <chuck@leoninepublicaffairs.com>
Sent: Friday, June 29, 2018 12:41 PM
To: Kriger, Ryan
Subject: Re: First Hearing on Protecting the Privacy of Vermonters

Thanks Ryan

Charles Storrow
Leonine Public Affairs, LLP
(802) 371-7863 (mobile)
Chuck@leoninepublicaffairs.com

On Jun 29, 2018, at 12:34 PM, Kriger, Ryan <ryan.kriger@vermont.gov> wrote:

I spoke too soon – the Office of has decided to push back the first hearing date in order to give people more time to prepare. The new date is **Monday, August 8, 9 am to 12 pm EST**, same location.
Please feel free to contact me with any questions or concerns.
-Ryan

From: Kriger, Ryan
Subject: First Hearing on Protecting the Privacy of Vermonters
I am writing to inform you of the first of a series of hearings to consider recommendations for legislative proposals to protect the privacy of Vermonters. You are receiving this email because your input into this discussion would be very valuable, and we seek to hear from a wide spectrum of voices in considering how best to proceed in this area. As you may know, Vermont takes the privacy and protection of its citizens very seriously and we seek to strike a balance between the need to protect our consumers and the needs of the business community to continue to develop a robust economy.
The hearing will take place on Thursday, July 12, from 1:00 - 4:00 pm at 29 Church Street, 3rd Floor in Burlington, Vermont (best entrance for the public is located at 110 Cherry Street). If you have any questions or concerns ahead of time, please feel free to email me or call me at 802-828-3170.
Topics under consideration will include, but not be limited to:

- Adoption of regulations concerning telecommunications privacy and whether to model such rules after the FCC's 2016 Privacy Order, WC Docket No. 16-106, FCC 16-148, adopted Oct. 27, 2016. The request for this recommendation was made in Act 66 of 2017.
- Whether Vermont should designate a Chief Privacy Officer, and what the responsibilities of that Officer would be. This request was made in Act 171 of 2018.
- Whether to regulate businesses that handle the data of consumers with whom they have a direct relationship, as requested in Act 171.
- Questions, concerns, and recommendations regarding the implementation of the Data Broker Registry, as authorized in Act 171.
- Changes that should be made to Vermont's Security Breach Notice Act, 9 V.S.A. § 2453.
- Questions or concerns regarding the State of Vermont's handling of citizen's data.
- Laws and regulations that can be adopted to encourage the growth of privacy-oriented technology companies in Vermont.
- The necessity of any additional approaches to protecting the data security and privacy of Vermont consumers.

If you do not want to receive further emails or know of others who should be on this list, please reply or email ago.datasecurity@vermont.gov.

Thank you,
Ryan

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

<August Meeting Press Release - FINAL.pdf>

Kriger, Ryan

From: Will Castleberry <wcastleberry@fb.com>
Sent: Tuesday, April 24, 2018 6:13 PM
To: Kriger, Ryan
Cc: Curtis, Christopher
Subject: Re: AG Letter to Facebook

Hey Ryan

We are finishing the letter now and should have it out to you very soon (days not weeks). Let me get back to you with a more firm date.

Will
202.420.0173

From: "Kriger, Ryan" <ryan.kriger@vermont.gov>
Date: Tuesday, April 24, 2018 at 5:34 PM
To: Will Castleberry <wcastleberry@fb.com>
Cc: "Curtis, Christopher" <Christopher.Curtis@vermont.gov>
Subject: AG Letter to Facebook

Will,

I hope you are well. As you are aware, a group of Attorneys General, including Vermont, sent Facebook a letter in late March. Has any response been issued? If Facebook has sent out any sort of explanatory letter, could you provide us a copy?

Thanks,

Ryan

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

Kriger, Ryan

From: Kriger, Ryan
Sent: Tuesday, April 24, 2018 5:34 PM
To: Will Castleberry (wcastleberry@fb.com)
Cc: Curtis, Christopher
Subject: AG Letter to Facebook

Will,

I hope you are well. As you are aware, a group of Attorneys General, including Vermont, sent Facebook a letter in late March. Has any response been issued? If Facebook has sent out any sort of explanatory letter, could you provide us a copy?

Thanks,

Ryan

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

Kriger, Ryan

From: Charles Storrow <chuck@leoninepublicaffairs.com>
Sent: Tuesday, April 17, 2018 11:14 AM
To: Curtis, Christopher; jbkennedyllc@comcast.net; Bridget Morris; lkleinberg@socialsentinel.com
Cc: Kriger, Ryan
Subject: RE: 2018-04-13 Proposed Amendments (v5).docx

Dear Chris,
This is to get back to you relative to our client's position/thoughts on the language that you circulated with your email below.
Unfortunately, we cannot support this language. As has been our position all along the fundamental problem is the inclusion of data elements that are matters of public record and are widely available in the public domain, such as name, address, date of birth, place of birth and mother's maiden name. Moreover, being a compliance oriented business RELX/Lexis Nexis is concerned about the use of what it sees as vague terms such "categorized or otherwise combined" and "public information."
The company would greatly prefer if "personal information" be defined to mean data elements that are not matters of public record or generally available in the public domain.
We appreciate you having made this proposal and your efforts to address our concerns.
I would be happy to continue the discussion.
Thanks—Chuck Storrow

From: Curtis, Christopher <Christopher.Curtis@vermont.gov>
Sent: Friday, April 13, 2018 6:12 PM
To: Charles Storrow <chuck@leoninepublicaffairs.com>; jbkennedyllc@comcast.net; Bridget Morris <bmorris@vtlobbyists.com>; lkleinberg@socialsentinel.com
Cc: Kriger, Ryan <ryan.kriger@vermont.gov>
Subject: FW: 2018-04-13 Proposed Amendments (v5).docx
Dear Chuck, Jeanne, Bridget, and Liz:
Attached is the current draft proposed amendment(s) for discussion purposes and review. We continue to analyze this and are not presenting it at this point as a formal proposed amendment. We continue to seek stakeholder feedback and questions, concerns, etc. to any proposed revisions and we are providing this for your consideration as potential progress that may help to address some of the questions and concerns we have heard to date.
Please note a few minor edits since our conversation a few days ago (highlighted in yellow). We reserve the right to further clarify key points and/or modify certain elements depending on additional feedback and/or internal review. We do hope that you will review this keeping in mind our continued good faith efforts to be responsive to stakeholder inquiry and feedback. Thank you for keeping the lines of communication open.
I hope this is generally helpful and that you all have a great weekend.
Best, Christopher
Christopher J. Curtis
State of Vermont
Office of the Attorney General
Chief, Public Protection Division
802-828-5586
christopher.curtis@vermont.gov

From: Kriger, Ryan
Sent: Friday, April 13, 2018 5:48 PM
To: Curtis, Christopher <Christopher.Curtis@vermont.gov>
Subject: 2018-04-13 Proposed Amendments (v5).docx

Kriger, Ryan

From: Charles Storrow <chuck@leoninepublicaffairs.com>
Sent: Friday, April 13, 2018 6:52 PM
To: Curtis, Christopher
Cc: jbkennedyllc@comcast.net; Bridget Morris; lkleinberg@socialsentinel.com; Kriger, Ryan
Subject: Re: 2018-04-13 Proposed Amendments (v5).docx

Chris, thanks. I've sent it on to our client and will be in touch. Chuck

Charles Storrow
Leonine Public Affairs, LLP
(802) 371-7863 (mobile)
Chuck@leoninepublicaffairs.com

On Apr 13, 2018, at 6:11 PM, Curtis, Christopher <Christopher.Curtis@vermont.gov> wrote:

> Dear Chuck, Jeanne, Bridget, and Liz:
> Attached is the current draft proposed amendment(s) for discussion purposes and review. We continue to analyze this and are not presenting it at this point as a formal proposed amendment. We continue to seek stakeholder feedback and questions, concerns, etc. to any proposed revisions and we are providing this for your consideration as potential progress that may help to address some of the questions and concerns we have heard to date.
> Please note a few minor edits since our conversation a few days ago (highlighted in yellow). We reserve the right to further clarify key points and/or modify certain elements depending on additional feedback and/or internal review. We do hope that you will review this keeping in mind our continued good faith efforts to be responsive to stakeholder inquiry and feedback. Thank you for keeping the lines of communication open.
> I hope this is generally helpful and that you all have a great weekend.
> Best, Christopher
> Christopher J. Curtis
> State of Vermont
> Office of the Attorney General
> Chief, Public Protection Division
> 802-828-5586
> christopher.curtis@vermont.gov
>
>
> **From:** Kriger, Ryan
> **Sent:** Friday, April 13, 2018 5:48 PM
> **To:** Curtis, Christopher <Christopher.Curtis@vermont.gov>
> **Subject:** 2018-04-13 Proposed Amendments (v5).docx
>
> <2018-04-13 Proposed Amendments (v5).docx>

Kriger, Ryan

From: Kriger, Ryan
Sent: Thursday, April 12, 2018 1:39 PM
To: Cuciti, Kimberly; Nick Sherman
Subject: RE: H.764 - VIC

Kim,

Could you give me a call? We have language that might work. 802-828-3170

-R

From: Cuciti, Kimberly <kimberly@egov.com>
Sent: Thursday, April 12, 2018 11:50 AM
To: Kriger, Ryan <ryan.kriger@vermont.gov>; Nick Sherman <nick@leoninepublicaffairs.com>
Subject: Re: H.764 - VIC

Hi Ryan,

Thank you for your response and time. My team can be available at 1:00. If that is ok, I can send out a conference line for everyone to attend.

Thanks,
Kim

From: "Kriger, Ryan" <ryan.kriger@vermont.gov>
Date: Thursday, April 12, 2018 at 11:32 AM
To: Nick Sherman <nick@leoninepublicaffairs.com>
Cc: "Cuciti, Kimberly" <kimberly@egov.com>
Subject: RE: H.764 - VIC

I just saw this. I can speak now, or the rest of my day other than the noon hour is free.

From: Nick Sherman <nick@leoninepublicaffairs.com>
Sent: Thursday, April 12, 2018 10:48 AM
To: Kriger, Ryan <ryan.kriger@vermont.gov>
Cc: Cuciti, Kimberly <kimberly@egov.com>
Subject: H.764 - VIC

Hi Ryan,

You may have met but I'd like to introduce Kim Cuciti, General Manager at VIC, who is copied on this email.

VIC has some concerns with the Attorney Generals office proposed revisions to H.764. I mentioned to Chris Curtis this morning that we would appreciate the opportunity to jump on the phone with you guys to discuss. VIC's legal folks would like to run their concerns by you.

Chris said that would be ok and asked that I email you. I know you are trying to move fast so I copied Kim on this email in hopes that if you are willing to jump on a call you can coordinate directly and I don't have to be a bottleneck.

Would that work?

Please let us know,

Thanks!

Nick Sherman

Kriger, Ryan

From: Kriger, Ryan
Sent: Thursday, April 12, 2018 11:55 AM
To: Cuciti, Kimberly; Nick Sherman
Subject: RE: H.764 - VIC

Sounds good, thank you.

-Ryan

From: Cuciti, Kimberly <kimberly@egov.com>
Sent: Thursday, April 12, 2018 11:50 AM
To: Kriger, Ryan <ryan.kriger@vermont.gov>; Nick Sherman <nick@leoninepublicaffairs.com>
Subject: Re: H.764 - VIC

Hi Ryan,

Thank you for your response and time. My team can be available at 1:00. If that is ok, I can send out a conference line for everyone to attend.

Thanks,
Kim

From: "Kriger, Ryan" <ryan.kriger@vermont.gov>
Date: Thursday, April 12, 2018 at 11:32 AM
To: Nick Sherman <nick@leoninepublicaffairs.com>
Cc: "Cuciti, Kimberly" <kimberly@egov.com>
Subject: RE: H.764 - VIC

I just saw this. I can speak now, or the rest of my day other than the noon hour is free.

From: Nick Sherman <nick@leoninepublicaffairs.com>
Sent: Thursday, April 12, 2018 10:48 AM
To: Kriger, Ryan <ryan.kriger@vermont.gov>
Cc: Cuciti, Kimberly <kimberly@egov.com>
Subject: H.764 - VIC

Hi Ryan,

You may have met but I'd like to introduce Kim Cuciti, General Manager at VIC, who is copied on this email.

VIC has some concerns with the Attorney Generals office proposed revisions to H.764. I mentioned to Chris Curtis this morning that we would appreciate the opportunity to jump on the phone with you guys to discuss. VIC's legal folks would like to run their concerns by you.

Chris said that would be ok and asked that I email you. I know you are trying to move fast so I copied Kim on this email in hopes that if you are willing to jump on a call you can coordinate directly and I don't have to be a bottleneck.

Would that work?

Please let us know,

Thanks!

Nick Sherman

Kriger, Ryan

From: Kriger, Ryan
Sent: Thursday, April 12, 2018 11:32 AM
To: Nick Sherman
Cc: Cuciti, Kimberly
Subject: RE: H.764 - VIC

I just saw this. I can speak now, or the rest of my day other than the noon hour is free.

From: Nick Sherman <nick@leoninepublicaffairs.com>
Sent: Thursday, April 12, 2018 10:48 AM
To: Kriger, Ryan <ryan.kriger@vermont.gov>
Cc: Cuciti, Kimberly <kimberly@egov.com>
Subject: H.764 - VIC

Hi Ryan,

You may have met but I'd like to introduce Kim Cuciti, General Manager at VIC, who is copied on this email.

VIC has some concerns with the Attorney Generals office proposed revisions to H.764. I mentioned to Chris Curtis this morning that we would appreciate the opportunity to jump on the phone with you guys to discuss. VIC's legal folks would like to run their concerns by you.

Chris said that would be ok and asked that I email you. I know you are trying to move fast so I copied Kim on this email in hopes that if you are willing to jump on a call you can coordinate directly and I don't have to be a bottleneck.

Would that work?

Please let us know,

Thanks!

Nick Sherman

Kriger, Ryan

From: Nick Sherman <nick@leoninepublicaffairs.com>
Sent: Thursday, April 12, 2018 10:48 AM
To: Kriger, Ryan
Cc: Cuciti, Kimberly
Subject: H.764 - VIC

Hi Ryan,

You may have met but I'd like to introduce Kim Cuciti, General Manager at VIC, who is copied on this email.

VIC has some concerns with the Attorney Generals office proposed revisions to H.764. I mentioned to Chris Curtis this morning that we would appreciate the opportunity to jump on the phone with you guys to discuss. VIC's legal folks would like to run their concerns by you.

Chris said that would be ok and asked that I email you. I know you are trying to move fast so I copied Kim on this email in hopes that if you are willing to jump on a call you can coordinate directly and I don't have to be a bottleneck.

Would that work?

Please let us know,

Thanks!

Nick Sherman

Kriger, Ryan

From: Charles Storrow <chuck@leoninepublicaffairs.com>
Sent: Wednesday, January 24, 2018 2:48 PM
To: Curtis, Christopher; Kriger, Ryan
Subject: Data Brokers

Dear Chris and Ryan,

This is to follow up on my conversation at lunch with you, Chris, concerning the data brokers legislation.

First off, I want to thank you for the proposal you gave to me yesterday. I know it is a "big give" and it is much appreciated. I am nonetheless asking for a couple of more changes.

First, would you agree to change the definition of "data brokers" or, at a minimum, narrow the requirement to file a statement with the SofS to DBs that collect and sell non-public records information, e.g., non-consumer facing companies that handle data used for marketing purposes? The vast majority of data handled by our client, RELX/LexisNexis, is gathered from public records. Most Vermonters know that things like criminal records, information related to owning real property, DMV motor vehicle operating records, etc., are a matter of public record.

Secondly, would you agree to refine and narrow the data elements that make up PI to exclude those elements that are readily available in the public realm? It seems incongruous that a DB would have to disclose on its annual filing with the SofS whether it suffered a breach of PI if the breach involved information, like peoples' names, that is widely available. One thought I have in this regard, which I would need to talk to my client about but which I throw out for your consideration is that a data breach be considered a PI breach if *more* than one data elements listed in the bill draft's definition of PI is acquired via the breach.

If you could let me know your thoughts on the foregoing it would be appreciated.

Thanks—Chuck Storrow

Charles Storrow, Partner
Leonine Public Affairs, LLP
1 Blanchard Court, Suite 101
Montpelier, VT 05602
Cell: (802) 371-7863 – Direct Office: 802-552-4470

chuck@leoninepublicaffairs.com
http://www.leoninepublicaffairs.com/

LEONINE
PUBLIC AFFAIRS

Kriger, Ryan

From: Jeanne Kennedy <jbkennedyllc@comcast.net>
Sent: Tuesday, January 23, 2018 10:41 AM
To: Curtis, Christopher
Cc: Charles Storrow; Kriger, Ryan
Subject: Re: 2018-01-22 Data Brokers New Clearinghouse Language.docx

Thank you

Sent from my iPhone

On Jan 23, 2018, at 10:25 AM, Curtis, Christopher <Christopher.Curtis@vermont.gov> wrote:

> Hi Chuck/Jeanne,
> Please find conceptual language attached. This would obviate the need for data broker data breach notification section in the bill. Thanks for your consideration.
> Best, Christopher
> Christopher J. Curtis
> State of Vermont
> Office of the Attorney General
> Chief, Public Protection Division
> 802-828-5586
> christopher.curtis@vermont.gov
> PRIVILEGED & CONFIDENTIAL COMMUNICATION: This communication may contain information that is privileged, confidential, and exempt from disclosure under applicable law. DO NOT read, copy or disseminate this communication unless you are the intended addressee. If you are not the intended recipient (or have received this E-mail in error) please notify the sender immediately and destroy this E-mail. Please consider the environment before printing this e-mail.
>
> **From:** Kriger, Ryan
> **Sent:** Monday, January 22, 2018 11:12 AM
> **To:** Curtis, Christopher <Christopher.Curtis@vermont.gov>
> **Subject:** 2018-01-22 Data Brokers New Clearinghouse Language.docx
>
> <2018-01-22 Data Brokers New Clearinghouse Language.docx>

Kriger, Ryan

From: Nick Sherman <nick@leoninepublicaffairs.com>
Sent: Thursday, January 18, 2018 3:55 PM
To: Kriger, Ryan
Subject: VIC Data Broker Language
Attachments: Edits Data broker legislation-1.docx

Hi Ryan,

Please find attached the proposed change to the data broker bill that VIC would like to request.

As an agent of the state that does not own any of the data (its all the state's data, VIC just processes it) they would like clarification that they are exempt from requirements of the data broker bill.

If this language is problematic we would be happy to discuss other options.

I will see you tomorrow.

All the best,

Nick Sherman

Get Outlook for iOS

Proposed Language to Exempt State Web Portal Vendor from Data Broker Legislation

In Section 2 of Draft 6.1 of the Commerce Committee Bill entitled "An Act Relating to Data Brokers and Consumer Protection" amend the definition of "business" to exclude a vendor acting on behalf of the state (page 12, line 3 of Draft 6.1.)

Proposed Language:

"Business" means a sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but in no case shall it include the State, a State agency, or any political subdivision of the State, *or a vendor acting on behalf of the state, state agency, or any political subdivision of the state.*

Kriger, Ryan

From: Charles Storrow <chuck@leoninepublicaffairs.com>
Sent: Friday, December 15, 2017 4:42 PM
To: Kriger, Ryan
Cc: Curtis, Christopher
Subject: Re: Data Broker Working Group

Thank you.

Charles Storrow
Leonine Public Affairs, LLP
(802) 371-7863 (mobile)
Chuck@leoninepublicaffairs.com

On Dec 15, 2017, at 4:31 PM, Kriger, Ryan <ryan.kriger@vermont.gov> wrote:

> Chuck,
> Per your request, the Data Broker Working Group report is attached.
> -R
> **Ryan G. Kriger**
> Assistant Attorney General
> Vermont Office of the Attorney General
> Public Protection Division
> 109 State Street
> Montpelier, VT 05609-1001
> ph: (802) 828-3170
> ryan.kriger@vermont.gov
>
> <2017-12-15 Data Broker Working Group Report.pdf>

Kriger, Ryan

From: Kriger, Ryan
Sent: Friday, December 15, 2017 4:32 PM
To: Charles Storrow
Cc: Curtis, Christopher
Subject: Data Broker Working Group
Attachments: 2017-12-15 Data Broker Working Group Report.pdf

Chuck,

Per your request, the Data Broker Working Group report is attached.

-R

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

Report to the General Assembly of the Data Broker Working Group issued pursuant to Act 66 of 2017

December 15, 2017

Issued by
Office of the Attorney General
Department of Financial Regulation

Table of Contents

I. Preamble 1

II. Executive Summary 1

III. Background 3

A. Legislative Mandate and the Working Group's Process 3

B. The Data Broker Industry is an Important and Growing Component of the Economy 3

C. The Equifax Breach Highlighted both the Risks of Data Aggregation and the Extent of Public Concern Associated with it 5

D. Benefits of the Data Broker Industry 6

E. There are Significant Risks Associated with the Widespread Aggregation and Sale of Data about Individuals by Data Brokers 7

F. Security Breaches 10

G. Past investigations into the Data Broker Industry 12

IV. Current Regulatory and Legal Background 13

A. Federal Protection of Consumers 13

B. State Protection of Consumers 14

C. Areas Subject to Both State and Federal Regulation 15

D. State Laws Without Direct Federal Counterparts 17

E. Federal Laws Without Direct State Counterparts: 18

F. The European Regulatory Regime: 20

G. Proposed legislation at the federal level or in other states 22

V. Recommendations 23

A. Definition of "Data Broker" 23

B. Regulation of Data Brokers 24

1. Credit Freeze Fee 25

2. Increase Consumer Awareness of Data Broker Opt-Out Rights 25

3. Prohibit Acquisition of Data for Illegal Purposes 26

4. Minimum Data Security 27

5. Swift Notice of Security Breaches 28

6. Protecting Children 29

Bibliography 30

Exhibit A: Stakeholder Recommendations i

Exhibit B: Massachusetts Data Security Regulation vi

I. Preamble

Information collection in commerce benefits consumers and industry. The bargain is that consumers provide information in exchange for transactional ease. Industry, on the other hand, not only acquires and possesses that information, in some cases, it transforms and commodifies the information. As a result, industry may facilitate not just the initial consumer transaction, but other transactions as well. This may lead to additional economic activity, but it also may pose risks to consumers who are unaware of secondary transactions involving the information they provide.

Data Brokers are businesses that collect personal data in order to resell it to third-parties. Vermont's citizens and the General Assembly have expressed concerns about practices within the Data Broker industry and possible harms that could arise from their activities. This report proposes for the Legislature's consideration several potential responses to these concerns, while also recognizing the importance of commercial transactions in the information economy.

II. Executive Summary

The Working Group convened under Act 66 of 2017 — comprising the Attorney General's Office and the Department of Financial Regulation — has studied the data-broker industry, heard extensive testimony in public meetings, and received written comments. It makes the following recommendations to the General Assembly for legislation that would protect Vermonters — particularly Vermont's most vulnerable — from the potential harms posed by the widespread storage and sale of sensitive data.

The Working Group, in making these recommendations, recognizes that the Data Broker industry includes many reputable companies that are crucial to the modern economy and are already making many efforts to protect consumers' data and privacy. The recommendations seek to impose minimal burdens on the industry as a whole, while also fulfilling state government's vital, longstanding role in protecting consumers.

The Working Group recommends the following definition of "Data Broker":

> A commercial entity that (1) assembles, collects, stores, or maintains personal information concerning individuals who are not customers or employees of that entity, and (2) sells the information to third parties.

Several types of businesses are not included in this definition. They are set forth in § V.A. The Assembly may decide to make these exemptions explicit.

The Working Group also recommends for consideration by the Legislature the following six potential actions that balance the benefits of the Data Broker industry with the potential harms of certain practices:

1) Amend Vermont's credit-freeze law (9 V.S.A. § 2480h) to prohibit credit reporting agencies from charging a fee to freeze or unfreeze consumers' credit reports;
2) Provide consumers with more information about opt-out rights and how to exercise them, by requiring Data Brokers to provide the Secretary of State with certain information;
3) Create new causes of action, enforceable by a consumer or the Attorney General, against those who acquire data with the intent of committing certain wrongful acts;
4) Require Data Brokers to employ reasonable security methods to protect data;[1]
5) Require Data Brokers that suffer certain data breaches to quickly provide notice of the breach; and
6) Protect children by prohibiting the sale of data about certain minors without parental consent.

While further legal analysis and discussion is required, the Working Group's preliminary research and legal analysis indicates that the litigation risk involved in the first three considerations is relatively low. The latter three may involve more substantial risks that the Assembly will want to carefully consider, in consultation with legislative counsel, DFR, and the AGO, in determining whether the potential benefits to the public outweigh the risks to the State.

[1] Note that Massachusetts has a data-security statute that applies to all businesses and is not limited to data brokers.

III. Background

A. Legislative Mandate and the Working Group's Process

In Act 66, the Vermont General Assembly directed the Attorney General's Office ("AGO") and the Department of Financial Regulation ("DFR") to study the data broker industry and potential regulation.[2] Specifically, the General Assembly asked the Working Group to submit a recommendation or draft legislation by December 15, 2017 that reflects (A) an appropriate definition of the term "data broker"; (B) whether and, if so, to what extent the Data Broker industry should be regulated by either DFR or the Attorney General; (C) additional consumer protections; and (D) proposed courses of actions that balance the industry's benefits with its actual and potential harms.[3]

Beginning in June 2017, DFR and AGO representatives formed a Working Group that met, studied the issue, and discussed potential regulatory solutions. The Working Group agreed that it was important to hear from all interested stakeholders before reaching any conclusions in the study.

The Working Group convened two days of public hearings in Burlington on July 25 and 26, 2017.[4] Representatives of industry trade groups, national Data Brokers, and local business[5] appeared and offered testimony, as did local, national, and international consumer and privacy advocates.[6] The Working Group also solicited and received written comments, and had several informal conversations with stakeholders.

B. The Data Broker Industry is an Important and Growing Component of the Economy

The Data Broker industry, generally speaking, is the group of businesses engaged in the acquisition, aggregation, analysis, and sale of information about individual consumers. The industry is, by a conservative estimate, a multibillion-dollar segment of the American economy, and growing.[7]

---

[2] 2017 Vt. Acts & Resolves No. 66, § 2. Copies of all documents referenced in this report have been stored in the Data Broker Working Group Document Repository, located at http://www.ago.vermont.gov/news-and-updates/data-broker-working-group1/data-broker-working-group-documents-referenced.php.

[3] *Id.*

[4] Video recordings of those hearings are available on the Attorney General's website, *at* http://ago.vermont.gov/focus/consumer-info/privacy-and-data-security1/data-broker-working-group.php

[5] Among those who testified were representatives from Acxiom, the Consumer Data Industry Association (CDIA), CompTIA, the Data and Marketing Association (DMA), MyWebGrocer, RELX (formerly Reed Elsevier, which owns LexisNexis), and TechNet.

[6] Among those who testified were representatives from Amnesty International, the Vermont Network Against Domestic & Sexual Violence, VT PIRG, and the World Privacy Forum, and a professor from Fordham University School of Law.

[7] *See* Senate Comm. On Commerce, Science & Transp., Staff Rep. for Chairman Rockefeller, Executive Summary, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, Dec. 18, 2013.

The Industry, by its nature, operates on a national scale, and has grown significantly in past decades due to advances in technology, including the internet and smart phones, increases in processing power, and decreases in data storage costs.

"Data Broker" or "Data Aggregator" is a broad term for a commercial entity whose primary line of business is the acquisition, aggregation, analysis, and resale of personal data. Data Brokers acquire a broad variety of information from a wide range of sources. For example, Data Brokers commonly gather data from: internet browsing history; online purchases; publicly available information (such as information maintained by state or local governments like property records, motor vehicle records, or court cases, or otherwise accessible information like social media connections and posts); location data; and registration or subscription information (such as magazine subscriptions or loyalty-card data from a grocery store). Data brokers also obtain information from federal and state government entities, by purchasing it from the source of the data (for example, from a social media website or blog, or from a brick and mortar store), and from other Data Brokers.

Data Brokers often combine data from several sources, allowing them to create extensive dossiers of information on individuals, sometimes including thousands of data points on a single person. Some Data Brokers focus primarily on collecting raw data from multiple sources, combining it, and "cleaning up" the data (i.e. confirming its accuracy). These data sets are then sold for use to various businesses.

Some Data Brokers also offer predictive analytics. Essentially, the Data Brokers apply algorithms to individuals' data based on correlations in data, and attempt to draw conclusions about consumers from their data. For example, based on the person's purchase history, online searches, social media "likes," and/or other inputs, a Data Broker might be able to extrapolate information about the individual's level of interest in a service or product, the individual's likelihood to purchase, physical or mental health, financial status, gullibility, tolerance for risk, addictions, or other likely attributes. The Data Broker can then add these conclusions to the data set and sell them as well. Consumer advocates have taken issue with the accuracy of these conclusions.[8]

Data Brokers sell information that is used for myriad business, government, and personal uses. The more prominent uses of information from Data Brokers include:

1) Targeted Marketing and Sales
    a) Mailing lists
    b) Telemarketing call lists
    c) Sales Staff Lead Generation
2) Targeted Online Advertising
3) Credit Reporting
4) Background Checks

[8] World Privacy Forum, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future*, April 2, 2014 ("Scoring of America").

5) Governmental Investigations
6) Risk Mitigation and Fraud Detection – confirming that individuals are who they say they are
7) People Search
8) Rate Setting by banks, insurers, or others that may require extensive information about a customer
9) Decisions by banks, insurers, or others as to whether to provide services
10) Ancestry Research
11) Voter Targeting and Strategy by political campaigns

Some Data Brokers target customer bases in certain industries. For example, a company might acquire data from a large Data Aggregator, and repackage that data and sell mailing lists to marketers. A Data Broker may sell specific products to law enforcement or to financial institutions for public protection or regulatory compliance purposes. Other Data Brokers might offer data products, such as People Search or Ancestry Research services, via a website or app for general usage.

C. The Equifax Breach Highlighted both the Risks of Data Aggregation and the Extent of Public Concern Associated with it

On September 7, 2017, Equifax Inc. announced that it experienced a security breach involving the information of 143 million U.S. Consumers (the number was subsequently updated to 145.5 million) ("2017 Equifax breach"). Equifax is one of the three major U.S. credit reporting agencies. The breach exposed the personal information of 247,607 Vermonters (roughly 40% of the state's population). The acquired data included names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, the breach exposed approximately 209,000 credit card numbers and dispute-related documents with information for approximately 182,000 U.S. consumers.

In the weekend immediately following the breach, Vermont's Consumer Assistance Program ("CAP") received over 700 complaints, the highest volume of complaints it has ever received relating to a single incident. The Working Group also heard numerous reports of citizens contacting their legislators, and several newspaper articles and opinion pieces were written about the incident.[9] The breach has prompted action by several Vermont legislators, including a well-attended November listening tour of the state by members of the Vermont Legislature, members of the Executive Branch, and others. The listening tour held public hearings in Springfield and Barton on Nov. 9, 2017; and Manchester Center and Burlington on Nov. 14, 2017.

[9] *E.g.* Manjoo, Farhad, *Seriously, Equifax? This Is a Breach No One Should Get Away With*, N.Y. Times, Sept. 8, 2017,https://www.nytimes.com/2017/09/08/technology/seriously-equifax-why-the-credit-agencys-breach-means-regulation-is-needed.html; Andriotis, AnnaMaria et al., *Senators Rip Credit-Reporting Model in Wake of Equifax Breach*, Wall St. J., Oct. 4, 2017, https://www.wsj.com/articles/senators-rip-credit-reporting-model-in-wake-of-equifax-breach-1507136171.

Vermont consumers primarily criticized Equifax for its lack of reasonable data security, delay in reporting the breach, and issues in responding to consumer concerns (including crashed websites, insufficient call center support, an initial attempt to force consumers to waive their right to trial in favor of arbitration, and a mistaken instruction that sent consumers to a fraudulent website). Another common criticism was that Equifax was collecting this data at all, and that consumers had no control over the data collection.

In addition to credit reporting, which is regulated by FCRA and FACTA, Equifax also engages in Data Broker activity that is not within the scope of those federal regulations. The breach came three months into the Working Group's study, after the hearings. The breach itself, and the media and citizen response to it, highlighted issues for the Working Group to consider, including:

- Public concern about third-party collection of personal data is far higher than it appeared to be prior to the breach;[10]
- Equifax's notification time after it first learned of the potential breach has received significant criticism, indicating that at least for certain types of breach, a more rapid response is expected;[11] and
- Despite public representations to the contrary,[12] some large, sophisticated data brokers have not implemented reasonable data security to protect consumer information.[13]

The Working Group also participated in the listening tour and has taken these observations into account when making its recommendations.

D. Benefits of the Data Broker Industry

The Data Broker Industry provides critical services to the modern economy. Consumer data collected and sold by Data Brokers is used for various purposes, including risk mitigation, marketing, and people search products.

Risk mitigation includes background checks used by law enforcement, potential employers, and landlords. It also includes fraud detection services used by businesses, like banks, that must verify the identity of the person with whom they are doing business.

Marketing products are used to connect businesses with potential customers. This includes traditional services like selling mailing lists to direct mail or door-to-door marketers, phone lists

---

[10] In addition to the complaint volume received by CAP, Attorney General T.J. Donovan reports that the Equifax breach is the most common issue he was asked about in the fall of 2017 when meeting with constituents.

[11] Vermont's Security Breach Notice Act requires notice of a breach "in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification . . ." 9 V.S.A. § 2435(b)(1).

[12] Stacy Cowley and Tara Bernard, *As Equifax Amassed Ever More Data, Safety was a Sales Pitch*, N.Y. Times, Sept. 23, 2017, https://www.nytimes.com/2017/09/23/business/equifax-data-breach.html.

[13] This observation is supported by data breaches involving other data brokers, which are explained in more detail in Section III.F.

to telemarketers, and lead generation to sales forces. These products are also used to send marketing emails and to serve up targeted advertisements on websites.

This final use is particularly important, because many "free" websites rely heavily on revenues derived from targeted advertising. The Working Group heard testimony during the public hearings that without targeted advertising and the revenues it provides, the "free internet" as we know it would cease to exist.

People search products have essentially replaced the traditional phone book as a way of locating individuals, but in a far more broad-based and global manner. People search can be used to research corporate executives and competitors, to find old acquaintances, to research one's family history and to find other information. People search products can offer much more information than available in the phone book, including the names of relatives, criminal background, interests/hobbies, and other information.

E. There are Significant Risks Associated with the Widespread Aggregation and Sale of Data about Individuals by Data Brokers

Generally, Data Broker activity poses risk of two types of harm to consumers: (i) those related to consumers' ability to know and control the data collected and sold about them, and (ii) those that arise from unauthorized access to consumers' information. Although other potential harms exist, it would be impractical to create legislation that would address every conceivable harm created by the free flow of data about individuals.[14]

Consumers' ability to know and control their data is important in large part because inaccuracies are widespread. In 2012 the FTC reported that 21% of consumers sampled had discovered a "confirmed material error" in one of the credit reports issued by the three major credit reporting bureaus, and 5.2% of consumers had successfully challenged a mistake that was serious enough to lower their credit score and burden them with higher interest rates. A person's data profile can become corrupted either by a bad actor or by mistake. Given the complexity of data collection, such mistakes are commonplace and, once made, can propagate as the erroneous data is sold and resold. This was a critical issue that state and federal governments tried to address with the first Fair Credit Reporting Acts, which allowed

---

[14] For example, the Working Group heard testimony regarding the general impact on human rights that arises from a loss of personal privacy, such as a tendency to self-censor when one is unsure who is listening, or the impact on human dignity that comes of knowing that strangers are being given insights into one's mental health, private predilections, or secret purchases. *See also e.g.*, United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, June 30, 2014.

Another, more concrete harm comes from the discrimination that consumers may experience, generally without knowing, when businesses acquire legally sold data sets that are supposed to be used for marketing, and use them for eligibility purposes that can lead to discriminatory pricing, redlining, or refusing opportunities. For example, a university might deny admission to an applicant based on an analytic score that is primarily derived from shopping patterns. *Scoring of America*. Not all Data Brokers permit this use, however, and industry representatives testified that they prohibit the use of marketing data for eligibility purposes.

consumers to inspect and correct their own data. These credit reports are the one subset of the Data Broker industry that is currently regulated by FCRA and FACTA.[15]

For data not regulated under FCRA, if a consumer is placed on an irrelevant mailing list or has other material mistakes in his or her profile, or a business is inspecting a consumer's profile to make pricing or employment decisions, such negative actions do not have to be reported to the consumer. As FTC Commissioner (and former Vermont Assistant Attorney General) Julie Brill explained, "If data broker profiles are based on inaccurate information or inappropriate classifications, or used for inappropriate purposes, the profiles have the ability to not only rob us of our good name, but also to lead to lost economic opportunities, higher costs, and other significant harm."[16] For example, a consumer might be refused the ability to obtain mobile phone services based on erroneous data in a profile. The consumer might have no idea why the transaction was blocked if the decision was based on non-FCRA data.[17]

Targeting Vulnerable Populations

Data Brokers frequently sell lists that group individuals by common characteristics. Some Data Brokers sell lists of individuals who may be at heightened risk of harm. While industry representatives have argued that there are legitimate marketing or other purposes for these lists, such lists can expose consumers to targeting by unscrupulous marketers and worse (e.g. stalkers, harassers, perpetrators of frauds). Data brokers have sold the following lists:[18]

- Rape survivors
- Addresses of Domestic Violence Shelters (which keep their locations secret under law)
- Police Officers' and State Troopers' home addresses
- Genetic Disease sufferers
- Senior citizens suffering from dementia
- HIV/AIDS sufferers
- People with addictive behaviors, and alcohol, gambling, and drug addictions
- People with diseases and prescriptions taken (including cancer and mental illness)
- Consumers who might want payday loans, including targeted minority groups
- People with low consumer credit scores

Stalking and Harassing

Information obtained from data brokers may make it easier for a stalker or harasser to locate an individual and keep tabs on their activity. Of particular concern here are certain new harms

---

[15] FTC, *Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003*, Dec. 2012.
[16] FTC, *Data Brokers, A Call for Transparency and Accountability*, Appendix C: Concurring Statement of Commissioner Julie Brill, May 27, 2014. ("FTC 2014 Report").
[17] *Id.*
[18] World Privacy Forum, *Testimony of Pam Dixon Executive Director, World Privacy Forum, Before the Senate Committee on Commerce, Science, and Transportation: What Information do Data Brokers Have on Consumers, and How Do They Use It?*, Dec. 18, 2013.

enabled by the ease of obtaining and spreading digital information, for example: *doxing* (publishing someone's contact information online so they can be harassed by others), and *swatting* (calling in a threat to have a SWAT team descend on a person's house).[19] While these or similar methods have been possible on a local level for years using phone books and other resources, the internet has made them far more prevalent and simultaneously far more harmful, due to the sheer number of people who can potentially perform them.

The National Network to End Domestic Violence provides guidance on how survivors can remove themselves from some Data Broker lists.[20] The Vermont Secretary of State maintains the "Safe at Home" program,[21] which allows victims of domestic violence, sexual assault, and stalking to obtain a substitute address to avoid being found. As of early 2017 the Vermont program had 138 participants.

The Working Group heard testimony from advocates as to the difficulty or impossibility of completely removing oneself from Data Broker lists. While some Data Brokers permit individuals to opt out of their databases, consumers often have no way to know whether they are in a specific database, or how to opt out. And, some Data Brokers do not allow opt-out at all.

Identity Theft, Scams and Fraud

Information obtained from a Data Broker also may make it easier for a bad actor to engage in identity theft or other forms of fraud because of the accessibility and comprehensiveness of information regarding an individual. Identity theft can harm the individual whose life is thrown into disarray, but also the businesses whom the ID Thief subsequently defrauds.

A few examples of such misuse of information acquired from data brokers:

- In 2013, it came to light that US Court Ventures, a Data Broker, had been selling data to an identity thief who then resold that data to other identity thieves on the dark web. During part of the period when this was happening, US Court Ventures was owned by Experian.[22]
- In 2016, the FTC settled a case with a Data Broker called Leap Lab that bought hundreds of thousands of payday loan applications containing Social Security and bank account

[19] Geoffrey A. Fowler, *Your Data is Way More Exposed than You Realize*, Wall St. J., May 24, 2017, https://www.wsj.com/articles/your-data-is-way-more-exposed-than-you-realize-1495657390; *see also* Anna North, *When a SWAT Team Comes to Your House*, N.Y. Times, Jul. 6, 2017, https://www.nytimes.com/2017/07/06/opinion/swatting-fbi.html;.

[20] Nat'l Network to End Domestic Violence, *People Searches and Data Brokers,* 2013, https://nnedv.org/mdocs-posts/people-searches-data-brokers/.

[21] https://www.sec.state.vt.us/safe-at-home.aspx.

[22] Brian Krebs, *Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records*, KrebsOnSecurity, Mar. 10, 2014, https://krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records/. *See also* Transcript of Waiver of Indictment and Plea to Information Hearing, U.S. v. Hieu Minh Ngo, Docket No. 1:12-cr-00144 Doc. 27, Mar. 7, 2014.

numbers, and then knowingly resold them to scammers, who emptied the accounts of millions of dollars.[23]

- The same year, the FTC obtained a default judgment against Sequoia One, LLC, another Data Broker that engaged in the same behavior.[24]
- Data Broker Information may be used for frauds other than identity theft. Information obtained from Epsilon in 2011, for example, was used in online fraud and spear-phishing attacks. (See Sec. III.F., below)

F. Security Breaches

Data brokers are a prime target for security breaches because they hold such large amounts of sensitive personal data aggregated in one place. The business community in general is subject to near-constant hacking attempts, and the Data Broker industry is no different. Even with reasonable security measures in place, some data breaches are inevitable. Accordingly, Vermont is one of 49 states with a Security Breach Notice Act, which requires businesses to notify consumers and the AGO or DFR when certain security breaches occur.[25] However, the type of acquired information that triggers the Act is very narrow, and information obtained in a breach of a Data Broker's site may not meet the requirements of the Act and may therefore be unreported. This leaves consumers vulnerable because they have not been informed that their information has been stolen.

For example, as discussed below, a breach involving usernames and passwords does not fall within Vermont's Act. A breach involving sensitive financial information or health information would not fall into the act if certain triggering data elements were not present. Finally, many Data Brokers claim to "aggregate, "anonymize," or "deidentify" data – in other words they store the data without a name, and therefore a breach including all of the data elements, but not the name, would not fall within the Act. The Working Group heard testimony that some Data Brokers may avoid storing information as PII, potentially limiting the efficacy of Vermont's

---

[23] Press Release, F.T.C., *Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers*, Feb. 18, 2016, www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive.

[24] Press Release, F.T.C., *FTC Puts An End to Data Broker Operation that Helped Scam More Than $7 Million from Consumers' Accounts*, Nov. 30, 2016, www.ftc.gov/news-events/press-releases/2016/11/ftc-puts-end-data-broker-operation-helped-scam-more-7-million.

[25] 9 V.S.A. § 2435. The Act only requires notice when the breached data includes "Personally Identifiable Information," defined in 9 V.S.A. § 2430(5) as an individual's first name or first initial and last name in combination with a:

(i) Social Security number;
(ii) motor vehicle operator's license number or nondriver identification card number;
(iii) financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; or
(iv) account passwords or personal identification numbers or other access codes for a financial account.

Notice Act with respect to Data Brokers. Moreover, numerous studies have shown that such data can easily be re-identified with an individual based on as few as three data elements.[26]

In addition to Equifax, a number of other large data brokers have experienced data breaches. These breaches involved sensitive information but were not subject to Vermont's Notice Act because they did not involve PII as defined in the Act. Published accounts of alleged data breaches are increasingly common:

- Acxiom, one of the largest Data Brokers, was hacked in 2003, and over a two-year period over 1.6 billion records were stolen, including names, addresses, and email addresses, some of which were sold to spammers.[27]

- Epsilon, a Data Broker that held email marketing lists for thousands of clients, experienced a breach in 2011 which exposed the name and email addresses of millions of individuals. The breached emails were used for spam, email fraud, and "spear-phishing," targeted email attempts to obtain user credentials.[28]

- RELX, the parent company of LexisNexis, has experienced multiple breaches, including one in 2005 in which the Social Security numbers, driver's license information, and address of 310,000 people may have been stolen,[29] one in 2009 involving 32,000 individuals,[30] and potentially one in 2013 in which millions of records were stolen and potentially resold on the Dark Web.[31] The last breach also allegedly involved thefts from Dun & Bradstreet and Kroll Background America.[32]

- Experian discovered a breach in 2015 involving 15 million records that belonged to T-Mobile but were stored on Experian's servers. The records were accessed over a 2-year

---

[26] L. Sweeney, *Simple Demographics Often Identify People Uniquely*. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. https://dataprivacylab.org/projects/identifiability/paper1.pdf; Natasha Singer, *With a Few Bits of Data, Researchers Identify 'Anonymous' People,* N.Y. Times., Jan. 29, 2015, https://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/.

[27] John Leyden, *Acxiom Database Hacker Jailed for 8 Years*, The Register, Feb. 23, 2006, https://www.theregister.co.uk/2006/02/23/acxiom_spam_hack_sentencing/. Vermont's Security Breach Notice Act did not take effect until 2005.

[28] Miguel Helft, *After Breach, Companies Warn of E-Mail Fraud*, N.Y. Times, Apr. 4, 2011, https://www.nytimes.com/2011/04/05/business/05hack.html; Brian Krebs, *Feds Indict Three in 2011 Epsilon Hack*, KrebsOnSecurity, Mar. 15, 2006, https://krebsonsecurity.com/2015/03/feds-indict-three-in-2011-epsilon-hack/.

[29] Heather Timmons, *Security Breach at LexisNexis Now Appears Larger*, N.Y. Times. , Apr. 13, 2005, https://www.nytimes.com/2005/04/13/technology/security-breach-at-lexisnexis-now-appears-larger.html.

[30] Angela Moscaritolo, *LexisNexis admits to another major data breach*, SC Magazine, May 4, 2009, https://www.scmagazine.com/lexisnexis-admits-to-another-major-data-breach/article/555843/.

[31] Juan Carlos Rodriguez, *LexisNexis Could Have Suffered Data Breach, FBI Says*, Law360., Sept. 26, 2013, https://www.law360.com/articles/475918/lexisnexis-could-have-suffered-data-breach-fbi-says; Brian Krebs, *Data Broker Giants Hacked by ID Theft Service*, KrebsOnSecurity, Sep. 25, 2013, https://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/.

[32] *Id.*

period and came from consumer applications for device financing and other services, and contained names, addresses, Social Security numbers, dates of birth, and additional information.[33]

Current law does not fully account for the modern reality of Data Brokers holding tremendous amounts of sensitive — but non-PII — data, or for the increasing number of breaches of that data.

G. Past investigations into the Data Broker Industry

Because the Data Broker Industry is largely opaque, much of the information we have about it comes from investigations by federal government entities or consumer organizations, and subsequently issued reports.[34] These reports have aided our analysis and can be found in the Document Repository.

For example:

In December 2013, the U.S. Senate Committee on Commerce, Science and Transportation released *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, under the direction of then-committee Chairman Senator John Rockefeller.

In April 2014, the World Privacy Forum, a non-profit public interest research and consumer education group, issued *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future*.

In May 2014, the Federal Trade Commission issued *Data Brokers: A Call for Transparency and Accountability*. This report was the result of a four-year study that began with the issuance of Orders to File Special Reports to nine data brokers pursuant to Section 6(b) of the FTC Act, 15 U.S.C. § 46(b), and included follow-up communications and meetings.

Also in May 2014, the Executive Office of the President, President's Council of Advisors on Science and Technology issued *Big Data and Privacy: A Technological Perspective*.

In May 2016, the Executive Office of the President issued *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*.

---

[33] Notice was provided for this breach, as it fell within the definition of Vermont's Notice Act.

[34] FTC 2014 Report, at i ("The Commission noted that, while the FCRA addresses a number of critical transparency issues associated with companies that sell data for credit, employment, and insurance purposes, data brokers within the other two categories remain opaque.").

IV. Current Regulatory and Legal Background

The following are the primary laws governing this area:[35]

- Federal Laws with no State Counterpart:
  - Fair and Accurate Credit Transactions Act (FACTA) is an amendment to FCRA that was added, primarily, to protect consumers from identity theft;
  - The Do Not Call List, implemented by the FTC's Telemarketing Sales Rule, allows consumers to opt out of receiving certain telemarketing calls;
  - The Health Insurance Portability & Accountability Act of 1996 (HIPAA) applies to health care providers and their business partners;
  - The Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act or GLBA) applies to financial institutions;
  - The Family Educational Rights and Privacy Act (FERPA) protects certain student information and applies to schools that receive federal funds;
  - The Children's Online Privacy Protection Act of 1998 (COPPA) applies to websites and mobile apps directed at children under 13; and
  - The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 gives guidance on what commercial email should include, and requires opportunities to opt out.
- State Laws with no Federal Counterpart:
  - Security Breach Notice Acts require notice to be given to consumers, and in some cases Attorneys General or other government actors, when a security breach occurs;
  - Social Security Number Protection Acts;
  - Safe Destruction of Documents Acts;
- Laws with State and Federal Counterparts:
  - Unfair and Deceptive Acts and Practices (UDAP) laws, including the Federal Trade Commission Act (and Vermont's Consumer Protection Act), are catch-all provisions that apply to a broad array of consumer protection issues;
  - The Fair Credit Reporting Act of 1970 (FCRA) applies to credit bureaus and those who provide information for, or use, credit reports;

A. Federal Protection of Consumers

The federal government has a number of privacy-related regulations, as described above, but they tend to be subject matter specific or "sectoral" – i.e., they regulate specific industries or activities. There is no single federal overarching privacy law. Because Data Brokers' activities tend to cut across sectors, they may be subject to an incomplete patchwork of regulation.

---

[35] As the Legislature is aware, in the fall of 2017, Legislative Council performed a comprehensive review of data-privacy regulation in general (i.e. not limited to data brokers) this fall. That review addressed some statutes and regulations that are beyond the scope of this report. The Review is available via the House Commerce & Economic Development Committee's website.

B. State Protection of Consumers

The State of Vermont has a long history of protecting its citizenry in the marketplace. The Consumer Protection Act (formerly called the Consumer Fraud Act, also sometimes called a "mini-FTC Act"), was enacted 50 years ago, in 1967.[36] Vermont's Fair Credit Reporting Act (or "mini-FCRA") was enacted in 1991.[37]

There are federal versions of these consumer protection laws. Specifically, Section 5 of the FTC Act (the "FTCA") parallels the Consumer Protection Act, and the Fair Credit Reporting Act is similar to Vermont's law. However, the FTCA does not preempt the CPA, and FCRA does not preempt Vermont's law. In fact, the federal FCRA contains express exclusions specific to Vermont's law.[38] Similarly, the Dodd–Frank Wall Street Reform and Consumer Protection Act,[39] which created the Consumer Financial Protection Bureau ("CFPB"), does not preempt the states' ability to regulate in the financial consumer protection area. Consequently, the states and federal government have long shared responsibility for regulating in this area, and frequently cooperate in enforcement actions.

The regulation of businesses that collect sensitive consumer data has also long been a domain of the states. The first Data Breach Notice Act was enacted in California in 2003.[40] Subsequently 48 other states and the District of Columbia adopted similar laws.[41] Vermont's Act was enacted in 2005. That same year, the General Assembly enacted laws regulating the use of Social Security numbers[42] and the safe destruction of documents containing personal information.[43] These laws are all housed in Chapter 62 of Title 9: Protection of Personal Information.

Chapter 62 is not limited to specific industries. There are no equivalent laws at the federal level.[44] Though, for example, data breach notification acts have been introduced in the U.S. Congress, the federal government has historically left regulation in this area to the States. There is no federal law that specifically regulates data brokers.

The areas where the US Government does address the collection and storage of sensitive information typically share enforcement authority with the States. For example, HIPAA

---

[36] 9 V.S.A. § 2453.
[37] 9 V.S.A. § 2480a.
[38] 15 U.S.C. § 1681t(b)(2).
[39] Enacted in 12 U.S. Code § 5491.
[40] California Civ. Code § 1798.82.
[41] A complete list of state data breach laws can be found at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[42] 9 V.S.A. § 2440.
[43] 9 V.S.A. § 2445.
[44] Federal laws address specific industries like health care (HIPAA), education (FERPA), and finance (GLBA), but there is no law of general applicability that addresses data breach, use of Social Security numbers, or safe destruction of information.

authorizes enforcement by state Attorneys General.[45] Graham-Leach-Bliley permits state laws that are not inconsistent, including state laws that offer greater protections than GLBA.[46]

In conclusion, regulation of Data Brokers is consistent with the State of Vermont's historic interest in protecting consumers and regulating use of sensitive data. As set forth in more detail below, certain types of legislation in this area would not conflict with federal law.

C. Areas Subject to Both State and Federal Regulation

Unfair and Deceptive Acts and Practices

The general prohibitions against Unfair and Deceptive Acts and Practices (UDAP) in commerce found in the Federal Trade Commission Act, 15 U.S.C. § 45, and Vermont's Consumer Protection Act, 9 VSA § 2435, have been applied to businesses for numerous violations of consumer privacy, including failure to provide reasonable data security to protect consumers' sensitive data[47] and failure to properly credential customers resulting in the sale of sensitive consumer data to identity thieves.[48]

An act is considered "unfair" if it causes or is likely to cause substantial injury to consumers, which is not reasonably avoidable by consumers themselves, and not outweighed by countervailing benefits to consumers or to competition. 15 U.S.C. § 45(n).

A "deceptive" act involves a material representation, omission, or practice that is likely to mislead consumers acting reasonably under the circumstances.

Fair Credit Reporting Act

The federal Fair Credit Reporting Act of 1970 (FCRA)[49] and Vermont's "mini-FCRA"[50] generally track each other, though Vermont's law varies in some ways that are expressly noted in the federal law. FCRA serves two main purposes: ensuring the accuracy of consumer-report information, and ensuring that only those with a legitimate business need for the information can access it.

FCRA applies to "consumer reporting agencies" (CRAs) that provide "consumer reports" for specific purposes.[51] A Data Broker might be a CRA for some lines of its business and not for

---

[45] This authority was created in the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, enacted in 42 U.S. Code § 1320d–5(d).
[46] 15 U.S.C. § 6807.
[47] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).
[48] *U.S. v. ChoicePoint, Inc.*, N. D. Ga. Docket No. 06-cv-0198 (2006).
[49] 15 USC § 1681 *et seq.* In 2003, FCRA was amended by the Fair and Accurate Credit Transactions Act (FACTA) (117 Stat. 1952, codified to 15 U.S.C. §§ 1681-1681x). This description of FCRA incorporates the FACTA amendments.
[50] 9 V.S.A. § 2480a-n.
[51] A consumer report is any written or oral communication that bears on a consumer's credit standing, credit-worthiness, credit capacity, character, general reputation, personal characteristics, or mode of living, if it used for

others. Similarly, a Data Broker might trade in data that qualifies as a "consumer report" as well as data that does not.

For example, the FTC has stated that data sold for marketing purposes, to detect fraud, or to locate people, does not fall within FCRA.[52] The three major credit bureaus, in issuing traditional credit reports, are covered by FCRA. However, the bureaus provide other services not covered by FCRA. The Working Group is not aware of any business whose entire slate of business services is regulated by FCRA.

FCRA imposes separate obligations on the "issuer" of a report (the CRA), the "user" of a report (the prospective creditor, insurer, landlord, or the like), and the "furnisher" of the information (the business that reports its experience with the consumer to the CRA for subsequent use in reports).

Under FCRA, issuers of reports must: (1) make their consumers reports available to consumers free once a year, (2) disclose on the report the identity of all parties receiving the information, (3) investigate any disputes a consumer raises, (4) correct or delete inaccurate information, and (5) have protections in place to ensure that the consumer has approved the dissemination of a report to a user.[53]

If a user of a credit report denies credit, insurance, or employment to a consumer based on information in the report, it must: (1) inform the consumer that the denial was due to information in the report; (2) provide the name and address of the report's issuer; and (3) notify the consumer of his or her right to receive a copy of the report and dispute its accuracy.

The creditor or other merchant who furnishes information to a CRA: (1) is prohibited from knowingly reporting information with errors to a CRA; (2) must correct any known errors; (3) must notify the CRA of any dispute the consumer has initiated; and (4) must investigate any disputed information and report any deletions of inaccurate information to all recipients of the inaccurate information.

Vermont's mini-FCRA primarily differs from federal law in that a consumer's consent for a business to release a credit report is generally assumed to apply to all affiliates of the business under federal law.[54] In Vermont, separate consent must be obtained for each affiliate.[55]

---

one of five "permissible purposes:" for credit, for employment, for insurance, to a governmental agency (e.g., for a license or other benefit), or to a person with a legitimate business need for the information in a transaction with the consumer. *Id.* A "consumer reporting agency" is defined as "any person which...regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties." *Id.*

[52] FTC 2014 Report at i.

[53] This is a description of key elements of FCRA, not the entirety of the obligations.

[54] 15 U.S.C. § 1681t.

[55] 9 V.S.A. § 2480e.

D. State Laws Without Direct Federal Counterparts

Security Breach Notice Acts

Forty-nine states, including Vermont,[56] have Security Breach Notice Acts, which require businesses and state entities to provide notice to consumers, and in Vermont to the AGO or DFR, when the business experiences a security breach. There is no equivalent federal law.

Security Breach Notice Acts apply when certain types of data ("Personally Identifiable Information" or "PII") is believed to have been improperly acquired. In Vermont, PII means a name or first initial and last name, when combined with: (i) Social Security number; (ii) motor vehicle operator's license number or nondriver identification card number; (iii) financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; or (iv) account passwords or personal identification numbers or other access codes for a financial account.

Vermont's Act requires businesses to notify the AGO or DFR of a breach within 14 business days of discovery of the breach, and to notify consumers in the most expedient time possible and without unreasonable delay, but no later than 45 days after the breach. The penalty for violating Vermont's Security Breach Notice is up to $10,000 per consumer.

Other states protect additional information such as a consumer's username and password, or biometric information. The applicability of such laws to security breaches in the Data Broker arena is more fully discussed in Section III.F.

Social Security Number Protection Act[57]

Vermont's Social Security Number Protection Act limits how businesses can use a consumer's Social Security Number (SSN). For example, they cannot: intentionally communicate someone's SSN to the public; require someone to transmit his or her SSN over the internet except via a secure or encrypted connection; print someone's SSN on a card used to access products or services; print someone's SSN on materials that are mailed to him or her (with some exceptions); or sell or disclose someone's SSN without written consent.

Document Safe Destruction Act[58]

Vermont's Document Safe Destruction Act requires businesses to take all reasonable steps to destroy consumers' records containing personal information by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or indecipherable.

---

[56] 9 V.S.A. §§ 2430-35.
[57] 9 V.S.A. § 2440.
[58] 9 V.S.A. § 2445.

This law exempts businesses subject to HIPAA, GLBA, and FCRA, described below.

California's Protections for Domestic Violence, Assault, and Stalking Victims

California, by statute, has created a program similar to Vermont's Safe at Home Program.[59] What is unique about California's statute is that it permits program participants to opt out of Data Broker databases. It also creates a private right of action for program participants against third parties who post or sell certain information about the participant online with the intent to cause harm to the participant,[60] with criminal penalties for persons who post information about program participants with intent to cause *imminent* harm.[61]

E. Federal Laws Without Direct State Counterparts:

The FTC's Telemarketing Sales Rule (TSR)[62] which implements the Do Not Call Registry[63]

The FTC's Do Not Call Registry is a list to which consumers may submit their telephone numbers. Telemarketers are generally prohibited from calling numbers on the Do Not Call Registry, with some exceptions. Telemarketers must check the registry every 31 days to confirm that no numbers on their call lists are in the registry. Political organizations, charities, surveyors, and businesses that have established a relationship with the consumer in the previous 18 months are excluded from this requirement.

Health Insurance Portability & Accountability Act of 1996 (HIPAA)

Under the statutory authority of HIPAA, the U.S. Department of Health & Human Services ("HHS") promulgated a Privacy Rule which controls how health care providers can share medical information. It limits with whom health care providers and other medical entities (called "covered entities") can share patients' medical information, and gives rights to patients to examine and copy their health records and to request corrections.[64]

Importantly, HIPAA puts controls on the covered entities, not on the data itself. In other words, it is legal for non-covered entities to trade in sensitive medical data, which can be acquired or extrapolated from sources other than covered entities.[65]

---

[59] Cal. Gov. Code § 6205 – 6210.
[60] *Id.* § 6208.1.
[61] *Id.* § 6208.2.
[62] 16 CFR 310; a thorough explanation of the TSR can be found at https://www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule; a guide for consumers can be found at https://www.consumer.ftc.gov/articles/0198-telemarketing-sales-rule.
[63] https://www.donotcall.gov/.
[64] 45 CFR Part 160; Part 164 Subparts A and E.
[65] FTC 2014 Report, fn 41; Adam Tanner, *How Data Brokers Make Money Off Your Medical Records*, Scientific American, Feb. 1, 2016, https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/.

Children's Online Privacy Protection Act of 1998 (COPPA)[66]

COPPA required that the FTC create a Rule (the COPPA Rule)[67] which gives parents control over what information is collected from young children online. The COPPA Rule applies to operators of websites and mobile apps that are directed to children under 13 that collect personal information from children, or general websites that have actual knowledge that they are collecting information from children under 13. These operators must:

- Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children;
- Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children;
- Give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents);
- Provide parents access to their child's personal information to review and/or have the information deleted;
- Give parents the opportunity to prevent further use or online collection of a child's personal information
- Maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security;
- Retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use.[68]

Federal Education Rights and Privacy Act (FERPA)

FERPA provides rights to parents to inspect and request corrections to students' education records. FERPA is administered by the U.S. Department of Education. The rights transfer to a student when he or she turns 18. FERPA also requires schools to obtain written permission from the parent or 18-year-old student before releasing information from the student's record.[69]

Schools may disclose "directory" information without consent, but must tell the parent/student first and give them the opportunity to opt out of the disclosure. Directory information includes name, address, telephone number, date and place of birth, honors and awards, and dates of attendance.[70]

---

[66] 15 U.S.C. § 6501–6505.
[67] 16 CFR Part 312.
[68] *See also* F.T.C., Complying with COPPA: Frequently Asked Questions, www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.
[69] 20 U.S.C. § 1232(g); 34 C.F.R. § 99.33.
[70] *Id.*

Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act or GLBA)

GLBA applies to financial institutions and requires disclosure of privacy policies, the right of consumers to opt out of sharing their data with nonaffiliated third parties, and prohibits the sharing of customer account numbers with nonaffiliated third parties for marketing purposes.

In addition, the Electronic Fund Transfer Act requires disclosures about data sharing when a consumer makes a fund transfer.[71] The Right to Financial Privacy Act prohibits some disclosures of financial records to the federal government.[72]

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003[73]

The CAN-SPAM statute, enforced by the FTC, is often listed as a privacy law but primarily gives businesses clear guidelines on what they can, cannot, and must do in email. Penalties for violation are up to $40,654 for each separate email. CAN-SPAM requires that for all commercial messages: header information cannot be false or misleading; subject lines cannot be deceptive; if the message is an ad it must be identified as such; the message must include the sender's physical postal address; the message must include instructions on how to opt out of future email; and opt-out mechanisms must continue work for at least 30 days after the messages is sent and opt-out requests must be honored within 10 days; and if another company is handling a business's email, the business must monitor what the other company is doing on its behalf.[74]

F. The European Regulatory Regime:

In May 2018, a significant privacy regulatory regime called the General Data Protection Regulation (GDPR) will begin to be enforced in the European Union (EU). Any Data Broker, wherever headquartered, if it has a European presence and collects or processes personal data from EU residents, or processes personal data on behalf of a business that holds EU residents' data, will be subject to the GDPR. The GDPR also applies to certain Data Brokers with no EU presence who target EU residents. This is noteworthy because Data Brokers who would be impacted by new Vermont regulations may soon be required to comply with EU regulations as far as EU Residents are concerned. The Working Group also believes it is useful to consider how a large, modernized, non-US jurisdiction is confronting these issues.

---

[71] 15 U.S.C. § 1693 *et seq.*
[72] 12 U.S.C. §§ 3401 – 3422.
[73] FTC Rule: 16 C.F.R. § 316.
[74] *See also* F.T.C., CAN-SPAM Act: A Compliance Guide for Business, https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

While the GDPR is too extensive to fully summarize here, its most notable features include:

- Citizens have a right to access any Personal Data[75] about them that is held by Data Controllers (an entity holding Personal Data), and to receive a free copy.
- Under certain circumstances, citizens may require Data Controllers to erase all data about the citizen; this is called "the right to be forgotten" or "data erasure."
- Before using a subject's personal data, the Data Controller must either obtain the subject's consent, and consent must be "freely given, specific, informed and unambiguous" or there must be a balancing of the individual's rights against the business interests of the Data Broker. The GDPR clarifies that "Silence, pre-ticked boxes or inactivity," is presumed inadequate to confer consent. The consent must also be specific to each data processing operation. In other words, if a business obtains a subject's consent to use data for one purpose, and then it or any downstream business wants to use it for a different purpose, it must obtain a separate consent from the subject. The use of Sensitive Personal Data requires "explicit consent," which is a higher requirement than standard consent.
- Parental consent is required before using data about children ages 16 and under, or a lower age (which can be determined by a member state).
- If a business uses scoring, it cannot solely rely on a computerized algorithm for decision-making if the decision can have a legal impact on individuals (such as a discriminatory impact)
- The GDPR includes standards of appropriate data protection of personal data, with higher standards for sensitive personal data.
- The GDPR requires notice of security breaches to the entity's country's "Supervisory Authority" within 72 hours of the breach involving any personal data.
- There are two levels of penalty under GDPR – violation of certain technical provisions, including breach notifications, permits fines up to the greater of 10 million euro (roughly $11.7M) or 2% of the company's prior year's global annual revenue. Other violations, including those relating to consent, permit fines of up to 20 million euro (roughly $23.3M) or 4% of the company's prior year's global annual revenue.

---

[75] "Personal Data," which is the key definition, is very broad, and means "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, IP address, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."

"Sensitive Personal Data," for which additional protections and restrictions apply, means "personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data."

G. Proposed legislation at the federal level or in other states

In response to heightened public concern regarding data security and privacy – prompted in part by the 2017 Equifax breach and other recent high-profile data-security incidents – legislatures and regulators across the country in recent years have considered, or are currently considering a variety of measures to protect consumers.

For example:

A number of states have enacted or are proposing legislation this year eliminating credit-freeze fees.[76]

In California, a bill relating to Data Brokers, SB-1348,[77] was introduced in 2014. This bill would have permitted consumers to review the information a Data Broker collected about the individual and to opt out of having that information shared. It required Data Brokers to clearly and conspicuously post their opt-out procedures. This bill did not pass.

Bill S.1815 was introduced in the U.S. Senate on September 14, 2017. This bill would give consumers the right to review and correct information collected by Data Brokers and to opt-out of sharing certain information for marketing purposes. The bill requires Data Brokers to establish procedures to ensure the accuracy of the information they collect and to implement comprehensive consumer privacy and data security programs. It also prohibits Data Brokers from obtaining personal information by false pretenses.

Previously, elements of this bill were introduced as S.668 in 2015 and S. 2025/H.R. 4516 in 2014. S.1995, introduced in 2014, addressed data breaches and also had data security standards language for Data Brokers. None of the bills have passed to date.

---

[76] The Working Group is aware of proposed legislation in at least three other states. There will likely be others. A complete list of current credit freeze laws can be found at http://www.ncsl.org/research/financial-services-and-commerce/consumer-report-security-freeze-state-statutes.aspx.

[77] Cal. Leg. SB-1348, Data brokers: sale of personal information (Feb. 21, 2014), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1348.

V. Recommendations

A. Definition of "Data Broker"

Act 66 requires the Working Group to propose "an appropriate definition of the term 'data broker.'"

The Working Group received a great deal of comment on the potential definition of the term. Many commenters suggested a narrow approach, to ensure that entities that hold data only incidentally — i.e. not as their primary business — would not be swept up.

The Working Group believes that any definition of data broker should encompass the following concepts:

1. A Data Broker is an entity that collects data about consumers, primarily for the purpose of selling that data or analytic scores based on that data.

   A Data Broker might take an interim step of analyzing, repackaging, cleaning, or otherwise manipulating the data, but the key element is that a data broker both collects and sells the data, and this is the primary purpose of the data collection.

2. A Data Broker does not have a direct relationship with the customer, user, or employee whose data is being collected.

   Some of the most prevalent consumer concerns about Data Brokers derive from the fact that consumers generally do not know who is handling their data, and cannot contact the data broker to have their information removed or corrected.

   Accordingly, the following businesses fall outside of the scope of the proposed definition of data broker, as the data they are collecting is from their own customers, and the customers therefore have some level of knowledge and control over the fact that their data is being collected, and the ability to opt out:[78]

   - Banks and other financial institutions
   - Utilities
   - Insurers
   - Retailers and Grocers
   - Restaurants and Hospitality Businesses
   - Social Media Websites and Mobile Apps

[78] In reality, often consumers may be unaware that the businesses with whom they directly do business are collecting and reselling their data, or to whom they are reselling it, or what the full implications of that resale are. Furthermore, many companies do not offer an "opt out," and given the widespread information sharing, any consumer attempting to avoid any business that resells his or her data would essentially have to opt out of e-commerce and use of the internet, which is not reasonable in the modern economy. However, for the purposes of focusing this legislation, the Working Group believes this distinction is important.

- Search Websites
- Businesses that provide services for consumer-facing businesses and maintain a direct relationship with those consumers, such as website, app, and e-commerce platforms

Working Group's Recommended Definition of "Data Broker"

A commercial entity that (1) assembles, collects, stores, or maintains personal information concerning individuals who are not customers, users, or employees of that entity, and (2) sells the information to third parties.

B. Regulation of Data Brokers

The Working Group recommends that the General Assembly consider adopting several measures that will provide consumers with significant protections, but will not place an undue burden on the Data Broker industry. The suggested legislation also addresses some of the current regulatory weaknesses that have been exposed by the Equifax breach. The Working Group also received additional recommendations for regulation through public comment, which are included in Exhibit A.

The Working Group recommends for the Legislature's consideration the following legislative potential actions:

1. Amend Vermont's credit-freeze law (9 V.S.A. § 2480h) to prohibit credit reporting agencies from charging a fee to freeze or unfreeze consumers' credit reports;
2. Provide consumers with more information about opt-out rights and how to exercise them, by requiring Data Brokers to provide the State of Vermont with certain information;
3. Create new causes of action, enforceable by a consumer or the Attorney General, against those who acquire data with the intent of committing certain wrongful acts;
4. Require Data Brokers to employ reasonable security methods to protect data;
5. Require Data Brokers that suffer certain data breaches to quickly provide notice of the breach;
6. Protect children by prohibiting the sale of data about certain minors without parental consent.

The first recommendation amends existing law. The latter parts should be added to Title 9 in Chapter 62: Protection of Personal Information.

While further legal analysis and discussion is required, the Working Group's preliminary research and legal analysis indicates that the litigation risk involved in the first three considerations is relatively low. The latter three may involve more substantial risks that the Assembly will want to carefully consider, in consultation with legislative counsel, DFR, and the

AGO, in determining whether the potential benefits to the public outweigh the risks to the State.

1. Credit Freeze Fee

Under current law, any Vermont consumer may place a security freeze on his or her credit report.[79] A credit reporting agency may not charge a fee to victims of identity theft, and for others may charge a fee of no more than $10.00 to freeze a report, and no more than $5.00 to remove the freeze. Requests to freeze credit reports must be made by certified mail. Victims of identity fraud must accompany the request with a copy of a police report, investigative report, or complaint that the consumer has filed with a law enforcement agency regarding the unlawful use of personal information.

The Working Group recommends that the General Assembly prohibit credit reporting agencies from charging a fee to any consumer who wishes to freeze or unfreeze his or her credit report. A victim of identity theft should not have to provide additional documentation of a theft to avoid paying a fee, as is required under current law. Such documentation is typically only available after a theft has occurred, and the real value of a credit freeze is to prevent identity theft, not to respond to it. Given that consumers rarely have a meaningful choice as to whether their data is collected, and it is largely the agencies who benefit from having the data, consumers should not have to pay the agencies for freezing and unfreezing their own data.

Three states already prohibit such fees: Indiana, Maine, and South Carolina.[80] Some states prohibit freeze fees for senior citizens. The Working Group understands that other states are currently considering legislation that would prohibit such fees. Federal legislation was proposed shortly after the 2017 Equifax breach, but it has not been enacted.

2. Increase Consumer Awareness of Data Broker Opt-Out Rights

One way to address consumer's privacy concerns is to better inform consumers of their opt-out rights. Several commenters recommended that the State provide an easier means for consumers to both learn about and exercise their opt-out rights.

Some Data Brokers already allow consumers to opt out of having their data shared. For example, the Data & Marketing Association (the "DMA"), a leading industry trade-group for data brokers, sets and maintains ethical guidelines for its members. *DMA Guidelines for Ethical Business Practice* ("DMA Guidelines").[81] The DMA Guidelines expressly state that: "A DMA Member: Honors requests not to have personally identifiable information transferred for marketing purposes."[82] Article 31 of the DMA Guidelines is to the same effect. Id. at 20. The

---

[79] 9 V.S.A. § 2480h.
[80] See Ind. Code § 24-5-24-14; Me. Rev. Stat. Tit. 10 § 1310(1)(A)(2); S. Carolina Code § 37-20-160(J).
[81] DMA, *Direct Marketing Association Guidelines for Ethical Business Practice*, https://thedma.org/wp-content/uploads/DMA-Guidelines-2016.pdf.
[82] *Id.* at 3.

Working Group heard testimony from both consumer advocacy groups and Data Brokers that requests for opt-out are generally honored.

However, most consumers do not know how to make such a request to the brokers that hold their data. Consumers, in fact, likely do not know who the brokers are, or how to go about contacting them and opting out of their lists. When the DMA testified before the House Commerce and Economic Development Committee, it was directly asked for a list of its membership and declined to provide one. Even when a consumer is aware of who holds their data, and how to contact them, it is difficult for a consumer to verify that their opt-out request has been honored.

To simplify this process and provide greater transparency for consumers, the Working Group recommends that Data Brokers be required annually to provide the following limited information to the State:[83]

1. The Data Broker's corporate name and primary physical, email, and web addresses.
2. If the Data Broker permits consumers to opt out of its databases or to opt out of certain sales of data:
    a. The method(s) for requesting the opt-out;
    b. If only certain sales are covered, which ones;
    c. Whether the Data Broker permits consumers to authorize a third-party to perform the opt-out in their stead.
3. If the Data Broker does not permit consumers to opt out, a statement that it does not permit opt-outs.

3. Prohibit Acquisition of Data for Illegal Purposes

One of the significant dangers of the broad availability of personal data is that it can be used with malicious intent to facilitate wrongful acts such as discrimination, stalking, harassment, fraud, or identity theft. While various criminal and civil statutes bar these practices, there is currently no prohibition on *acquiring* data for the purpose of committing these wrongful acts. The Working Group recommends that the General Assembly adopt legislation that would make it illegal to acquire personal data for the purpose of:

1. Stalking or harassing;
2. Identity theft;
3. Financial fraud;
4. Email fraud;
5. Employment discrimination; or
6. Housing discrimination.

[83] The Working Group has identified the Secretary of State as an official who currently performs a similar function in other areas (e.g. the Corporations Database) and may have an infrastructure to build on. The Working Group recommends that the Legislature consult with the Secretary of State regarding the resources required to securely and effectively implement this recommendation.

Creating a cause of action — enforceable by State's Attorneys, the Attorney General or consumers — will set a clear standard that bad actors should not use information garnered from data brokers to facilitate other wrongs. It will also provide an additional, earlier authority for the Attorney General or a consumer to take legal action to prevent the wrong before it happens.

4. Minimum Data Security

Even large and sophisticated Data Brokers can have deficient data security, as evidenced by the 2017 Equifax breach and other breaches described above. The Legislature should consider requiring expressly that data brokers must adequately secure sensitive data. To date, states[84] and the FTC have prosecuted unreasonable data security as an unfair or deceptive act under the FTC Act or state Consumer Protection Acts. One criticism of this approach is that it does not provide pre-violation guidance as to what "reasonable" data security is.

The Commonwealth of Massachusetts has addressed this issue by setting minimum data security standards, which apply to all businesses that handle certain highly sensitive personal information.[85] While Massachusetts has the most detailed standards, which are set forth in a regulation, fourteen other states have laws that generally require that businesses who handle personal information "implement and maintain reasonable security procedures" or similar requirements.[86] The Working Group proposes that Vermont consider adopting a standard similar to Massachusetts, either with regard to all businesses handling PII, or only with regard to Data Brokers.

In Massachusetts, any entity that owns or licenses personal information about any Massachusetts resident must "develop, implement, and maintain a comprehensive information security program that . . . contains administrative, technical, and physical safeguards" that are appropriate based on a variety of factors (size and type of business, nature and amount of data, available resources). The regulation requires compliance with any data security requirements applicable to the data or the entity holding it. The regulation also imposes more specific requirements concerning risk assessment, oversight of employees and contractors, employee

---

[84] Multistate enforcement actions regarding failure to adequately secure sensitive data have recently resulted in Assurances of Discontinuance with Target (48 States, available at https://ag.ny.gov/press-release/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation-over), Adobe Systems Inc. (15 states, available at http://www.illinoisattorneygeneral.gov/pressroom/2016_11/20161110.html), and Nationwide Mutual Insurance Company (34 states, available at http://ago.vermont.gov/focus/news/attorney-general-announces-nationwide-data-breach-settlement.php).

The State of Vermont has also entered into several non-Multistate settlements with businesses that failed to provide adequate security, including SAManage Inc. (available at http://ago.vermont.gov/focus/news/attorney-general-settles-data-breach-case-for-$264000-issues-$400-per-social-security-number-penalty.php) and Hilton Domestic Operating Company Inc.(available at http://ago.vermont.gov/focus/news/vermont-attorney-general-resolves-security-breach-with-hilton-company-to-pay-$300000-penalty.php)

[85] 201 Code of Mass. Regs. 17.01 – 17.05; *see* Mass. Gen. L. Ch. 93H, § 2(a) (authority for regulations).

[86] http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx

training, and the like. Finally, the regulation imposes even-more specific requirements on regulated entities' computer systems and access thereto. The Massachusetts standards have been in effect since 2010 and are reproduced in Exhibit B.

5. Swift Notice of Security Breaches

The Working Group recommends that the Legislature consider requiring Data Brokers to provide prompt notice when certain sensitive information is compromised by a security breach. Prompt notice of a breach is important so that consumers can take steps to protect themselves. Depending on the information that a Data Broker has, a Data Broker breach may be particularly sensitive because it will likely to lead to identity theft and fraud. Moreover, because Data Brokers' primary business is, by definition, the acquisition, storage, and sale of data, they may reasonably be held to a higher standard than other businesses that hold data only incidentally to their primary business.

Vermont's Security Breach Notice Act, 9 V.S.A. § 2435, is insufficient to address Data Broker breaches because it is only triggered when a data collector that owns or licenses computerized Personally Identifiable Information (PII)[87] is breached. For example, an entity that had the following types of data breached would not be required to report a breach under current Vermont law because the data is not PII:

- Name plus health care information, list of treatments (this information can be derived from purchase history and searches, and is also not covered by HIPAA);
- Name, address, phone, family history and names of relatives, income, assets, and liabilities; or
- Social security number, driver's license number, passport number, age, or address, without a name (however, such "deidentified" data can easily be re-connected with a name).

In addition, the Security Breach Notice Act requires notice "in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery."[88] Equifax provoked widespread outrage because many felt that the notice was given too late. The Working Group believes that it would be appropriate to strengthen the notice requirement for Data Brokers, given that their primary business is the acquisition, storage, and sale of data, and because of the potential harm to consumers associated with delay.

The Working Group does not recommend expanding the existing Vermont Notice Act, as that Act covers all businesses that collect data, not just Data Brokers. Data Brokers are differently situated from other businesses that hold sensitive data, and accordingly it is appropriate to regulate them differently. However, the proposed Data Broker Security Breach Notice Act should closely track the language of the Vermont Notice Act, for simplicity in implementation.

---

[87] Personally Identifiable Information is defined in fn 25.
[88] 9 V.S.A. § 2435(b)(1).

The Working Group recommends that the Legislature consider a Data Broker Security Breach Notice Act consistent with the existing Notice Act, except:

- Applies only to Data Brokers;
- Applies to breaches involving "Data Broker Personal Information" ("DBPI"), a definition which would draw from the broader PII definition found in FERPA;
- Requires notice to the Attorney General's Office;
- Requires that notice include a description of all categories of data acquired;
- Currently, under subpart (d)(1) of the Vermont Notice Act, a business that believes that "misuse of personal information is not reasonably possible" can notify the AGO or DFR and if the agency agrees with the determination, no notice will be necessary. The Data Broker version would also have the words "or the likelihood of identity theft is extremely low" or words to that effect.

6. Protecting Children

The Working Group heard testimony that protections for data about children are quite limited under current law. The Working Group's research confirms this to be the case.

Federal law covers some sharing of information about children, but the laws are limited in scope. As discussed above, FERPA addresses certain information about students collected by schools receiving federal funds, and requires parental consent for release of any such information for commercial purposes.[89] COPPA addresses information supplied to websites for children under 13.[90] However, there is no federal protection for non-school data about children between 13 and 18 years old, and no protections for data about children obtained through surveys, purchase history, write-in contests, or the like. Furthermore, if an unscrupulous website does collect a child's data in violation of the law, once the data is in the hands of data brokers its source or origin may be lost and there is nothing stopping the subsequent resale of that data.

The working group recommends that the Legislature consider prohibiting the sale of any sensitive data collected outside of school about children between the ages of 13 and 18 without the written permission of the child's parent or guardian, except for limited purposes. Because there are several potential areas of litigation risk, the Working Group recommends that the Legislature work closely with Legislative Council and the Attorney General's Office in drafting such legislation.

---

[89] See 20 U.S.C. § 1232g(b) (FERPA prohibition on certain releases of student data); 34 C.F.R. § 99.33 (regulatory description of FERPA limitation on disclosure of student information).

[90] See 15 U.S.C. § 6501(1) (COPPA definition of "child" as anyone under age 13); *id.* § 6502(d) (COPPA preempts state law only to the extent that it is inconsistent with the treatment of activities governed by COPPA). Because COPPA governs only activities involving children under 13 it does not preempt state laws concerning teenagers.

Bibliography

All documents have been archived at http://www.ago.vermont.gov/news-and-updates/data-broker-working-group1/data-broker-working-group-documents-referenced.php.

1. 2017 Vt. Acts & Resolves No. 66.

2. Adam Tanner, *How Data Brokers Make Money Off Your Medical Records*, Scientific American, Feb. 1, 2016, https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/.

3. Andriotis, AnnaMaria et al., *Senators Rip Credit-Reporting Model in Wake of Equifax Breach*, Wall St. J., Oct. 4, 2017, https://www.wsj.com/articles/senators-rip-credit-reporting-model-in-wake-of-equifax-breach-1507136171.

4. Angela Moscaritolo, *LexisNexis admits to another major data breach*, SC Magazine, May 4, 2009, https://www.scmagazine.com/lexisnexis-admits-to-another-major-data-breach/article/555843/.

5. Anna North, *When a SWAT Team Comes to Your House*, N.Y. Times, Jul. 6, 2017, https://www.nytimes.com/2017/07/06/opinion/swatting-fbi.html.

6. Brian Krebs, *Data Broker Giants Hacked by ID Theft Service*, KrebsOnSecurity, Sep. 25, 2013, https://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/.

7. Brian Krebs, *Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records*, KrebsOnSecurity, Mar. 10, 2014, https://krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records/

8. Brian Krebs, *Feds Indict Three in 2011 Epsilon Hack*, KrebsOnSecurity, Mar. 15, 2006, https://krebsonsecurity.com/2015/03/feds-indict-three-in-2011-epsilon-hack/.

9. Cal. Leg. SB-1348, Data brokers: sale of personal information (Feb. 21, 2014), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1348

10. Complaint, *Massachusetts v. Equifax* (Sept. 19, 2017), http://www.mass.gov/ago/docs/press/2017/equifax-complaint.pdf.

11. DMA, *Direct Marketing Association Guidelines for Ethical Business Practice*, https://thedma.org/wp-content/uploads/DMA-Guidelines-2016.pdf.

12. Exec. Office of the President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, May 2016.

13. Exec. Office of the President, President's Council of Advisors on Sci. and Tech., *Big Data and Privacy: A Technological Perspective*, May 2014.

14. F.T.C., CAN-SPAM Act: A Compliance Guide for Business, https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

15. F.T.C., Complying with COPPA: Frequently Asked Questions, www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

16. F.T.C., Complying with the Telemarketing Sales Rule, https://www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule

17. F.T.C., *Data Brokers, A Call for Transparency and Accountability*, May 2014.

18. F.T.C., *Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003*, Dec. 2012.

19. F.T.C., The Telemarketing Sales Rule, https://www.consumer.ftc.gov/articles/0198-telemarketing-sales-rule.

20. Farhad Manjoo, *Seriously, Equifax? This Is a Breach No One Should Get Away With*, N.Y. Times, Sept. 8, 2017, https://www.nytimes.com/2017/09/08/technology/seriously-equifax-why-the-credit-agencys-breach-means-regulation-is-needed.html.

21. Geoffrey A. Fowler, *Your Data is Way More Exposed than You Realize*, Wall St. J., May 24, 2017, https://www.wsj.com/articles/your-data-is-way-more-exposed-than-you-realize-1495657390.

22. Heather Timmons, *Security Breach at LexisNexis Now Appears Larger*, N.Y. Times., Apr. 13, 2005, https://www.nytimes.com/2005/04/13/technology/security-breach-at-lexisnexis-now-appears-larger.html.

23. John Leyden, *Acxiom database hacker jailed for 8 years,* The Register, Feb. 23, 2006, https://www.theregister.co.uk/2006/02/23/acxiom_spam_hack_sentencing/

24. Juan Carlos Rodriguez, *LexisNexis Could Have Suffered Data Breach, FBI Says*, Law360, Sept. 26, 2013, https://www.law360.com/articles/475918/lexisnexis-could-have-suffered-data-breach-fbi-says.

25. L. Sweeney, *Simple Demographics Often Identify People Uniquely*. Carnegie Mellon Univ., Data Privacy Working Paper 3. Pittsburgh 2000. https://dataprivacylab.org/projects/identifiability/paper1.pdf.

26. Miguel Helft, *After Breach, Companies Warn of E-Mail Fraud*, N.Y. Times, Apr. 4, 2011, Retrieved from https://www.nytimes.com/2011/04/05/business/05hack.html.

27. Nat'l Network to End Domestic Violence, *People Searches and Data Brokers,* 2013, https://nnedv.org/mdocs-posts/people-searches-data-brokers/.

28. Natasha Singer, *With a Few Bits of Data, Researchers Identify 'Anonymous'* People, N.Y. Times, Jan. 29, 2015, https://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/.

29. Press Release, F.T.C., *Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers,* Feb. 18, 2016, www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive.

30. Press Release, F.T.C., *FTC Puts An End to Data Broker Operation that Helped Scam More Than $7 Million from Consumers' Accounts*, Nov. 30, 2016, www.ftc.gov/news-events/press-releases/2016/11/ftc-puts-end-data-broker-operation-helped-scam-more-7-million.

31. Press Release, Ill. Att'y Gen., *Attorney General Madigan Announces $1 Million Settlement with Adobe*, Nov. 10, 2016, http://www.illinoisattorneygeneral.gov/pressroom/2016_11/20161110.html.

32. Press Release, N.Y. Att'y Gen., *A.G. Schneiderman Announces $18.5 Million Multi-State Settlement With Target Corporation Over 2013 Data Breach*, May 23, 2017, https://ag.ny.gov/press-release/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation-over.

33. Press Release, Vt. Att'y Gen., *Attorney General Announces Nationwide Data Breach Settlement*, Aug 9, 2017, http://ago.vermont.gov/focus/news/attorney-general-announces-nationwide-data-breach-settlement.php.

34. Press Release, Vt. Att'y Gen., *Attorney General Settles Data Breach Case for $264,000; Issues $400 Per Social Security Number Penalty*, Sep. 29, 2017, http://ago.vermont.gov/focus/news/attorney-general-settles-data-breach-case-for-$264000-issues-$400-per-social-security-number-penalty.php.

35. Press Release, Vt. Att'y Gen., *Vermont Attorney General Resolves Security Breach with Hilton Company to Pay $300,000 Penalty*, Oct. 31, 2017, http://ago.vermont.gov/focus/news/vermont-attorney-general-resolves-security-breach-with-hilton-company-to-pay-$300000-penalty.php.

36. Senate Comm. On Commerce, Science & Transp., Staff Rep. for Chairman Rockefeller, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, Dec. 18, 2013.

37. Stacy Cowley and Tara Bernard, *As Equifax Amassed Ever More Data, Safety was a Sales Pitch*, N.Y. Times, Sept. 23, 2017, https://www.nytimes.com/2017/09/23/business/equifax-data-breach.html.

38. Transcript of Waiver of Indictment and Plea to Information Hearing, *U.S. v. Hieu Minh Ngo*, Docket No. 1:12-cr-00144 Doc. 27, Mar. 7, 2014.

39. United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, June 30, 2014.

40. World Privacy Forum, *Testimony of Pam Dixon Executive Director, World Privacy Forum, Before the Senate Committee on Commerce, Science, and Transportation: What Information do Data Brokers Have on Consumers, and How Do They Use It?*, Dec. 18, 2013.

41. World Privacy Forum, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future,* April 2, 2014.

Exhibit A: Stakeholder Recommendations

This exhibit summarizes the recommendations made by stakeholders and interested parties through testimony and comments submitted to the Working Group.[91]

Some parties made recommendations that the Working Group have included in part or whole in its proposal to the General Assembly. A number supported the idea of a Data Broker Clearinghouse or registration with the state.[92] Some recommended that the state require Data Brokers to adhere to minimum security standards.[93] Two recommended a prohibition on the use of data to discriminate or otherwise break the law.[94]

Stakeholders also made the following recommendations that were not included in the Working Group's proposal.

1. No Legislative Change

Some stakeholders opined that no legislative change is necessary because the industry currently has sufficient self-regulation, industry members are aware of potential harms and have taken steps to mitigate those harms, and regulation could have harmful unintended consequences. These stakeholders did not propose any alternatives for legislators to consider.

This recommendation was made by Acxiom, the Coalition for Sensible Public Record Access (CSPRA); the Consumer Data Industry Association (CDIA); Computing Technology Industry Association (CompTIA); RELX Group (owner of LexisNexis); and TechNet.

2. Consumer Right to Know and Disclosures

The most common recommendations involved information that consumers should be allowed to discover about the Data Brokers that collect their data. Proposals suggested that Data Brokers should be required to either affirmatively disclose this information or make it available on request. Some recommendations related to general information about Data Brokers' practices, others to individual consumer rights regarding to their own specific data.

These commenters suggested that a Broker should be required to clearly and conspicuously disclose:

---

[91] All submitted comments can be found at http://ago.vermont.gov/focus/consumer-info/privacy-and-data-security1/data-broker-working-group.php.

[92] This recommendation was made by Consumer Action, Consumer Federation of America (CFA), Consumer Watchdog, the National Consumers League (NCA), PrivacyMate, Privacy Rights Clearinghouse, Prof. N. Cameron Russell of Fordham University School of Law, and the Vermont Public Interest Research Group (VPIRG).

[93] This recommendation was made by Consumer Action, CFA, Consumer Watchdog, NCA, PrivacyMate, and Privacy Rights Clearinghouse.

[94] This recommendation was made by Amnesty International and Prof. Chris Jay Hoofnagle of the University of California Schools of Information and School of Law.

- The names and contact information of third-parties with whom the Data Broker shares information;
- the purposes for which the information is sought and sold;
- the types of lists and "categories" of consumers that the Data Broker sells; and
- the sources of the information that the Data Broker collects.

These commenters also suggest that Data Brokers should be required to provide to any Consumer who requests it:

- a complete copy of all the information collected about the consumer;
- an audit or disclosure log to determine how data about the consumer has been sold and to whom;
- the various "categories" that the consumer has been assigned into and why.

These recommendations were made by the American Civil Liberties Union (ACLU), Amnesty International, Consumer Action, Consumer Federation of America (CFA), Consumer Watchdog, Prof. Chris Jay Hoofnagle of the University of California Schools of Information and School of Law, the National Consumers League (NCA), PrivacyMate, Privacy Rights Clearinghouse, Prof. N. Cameron Russell of Fordham University School of Law, and the Vermont Public Interest Research Group (VPIRG). This is a summary of the recommendations. Some of these stakeholders proposed a subset of the recommendations above.

3. Opt-Out

Several stakeholders recommended that Data Brokers be required to establish an opt-out procedure for sharing information with third-parties. Some advocated further that any such opt-out procedure be free-of-charge. Some stakeholders recommended this option be limited to data used for marketing purposes or people search products. One stakeholder recommended the opt-out be the default, and consumers have the option to opt in to allow Data Brokers to collect, store, and share their data.

The following recommendations would apply to either a newly created opt-out requirement, or to the existing opt-out procedures that some Data Brokers already have:

- Opting out be available to individuals in a one-step process encompassing all Data Brokers listed in the clearinghouse;
- No personal information provided to a Data Broker for the purpose of opting out may be used by the Data Broker to add to its profile on that individual; and
- Fees to opt out be prohibited.

These recommendations were made by the ACLU, CFA, NCA, Consumer Watchdog, Consumer Action, Vermont Consumer Assistance Program (a division of the Attorney General's Office that did not participate in the Working Group), the Vermont Network Against Domestic & Sexual Violence, PrivacyMate, and Privacy Rights Clearinghouse.

Privacy Rights Clearinghouse also recommended adoption of a law like one existing in California which provides participants in the Secretary of State's confidential address program, Safe at Home (for victims of domestic violence or stalking and reproductive health care providers, employees, and volunteers) with the right to demand the removal of their personal information, including home address and phone number, from online search engines or databases, and imposes related obligations on the operators of such search engines and databases. Cal. Gov. Code § 6208.1.

4. FCRA rights: Right to Review and Correct, and Adverse Action Reporting

Several stakeholders recommended that Data Brokers provide a method for consumers to review and correct information that the Data Brokers maintain about the consumers, similar to requirements under FCRA regarding credit reports. The comments recommend that instructions on how to exercise these rights should be clearly and conspicuously posted on each Data Broker's website.

Comments concerning this recommendation suggested that entities that decline to transact with a consumer based on information provided by a Data Broker for fraud mitigation purposes should be required to provide the consumer with a basic explanation of the nature of that data and how to reach the Data Broker that supplied it, similar to requirements under FCRA regarding adverse actions.

These recommendations were made by the ACLU, Amnesty International, CFA, NCA, Consumer Watchdog, Consumer Action, PrivacyMate, Privacy Rights Clearinghouse, and VPIRG.

5. Deidentification and Anonymization

Two stakeholders recommended that Data Brokers that de-identify data should be required to disclose their de-identification technique so that it is understandable, and further that there be a clear link established as to how this degree of de-identification protects privacy, and a disclosure of the perceived risk of re-identification.

These comments also suggest that legislation:

- Prohibit as deceptive the practice of calling data "anonymous" or de-identified where data brokers and their clients can re-identify or otherwise link the data to individuals;
- Prohibit data brokers from re-identifying datasets that were collected under promises of privacy or anonymity; and
- Prohibit data brokers from coaching clients to collect data in misleading ways (for an example, look at the reverse enhancement battle in California, where data brokers coached clients to collect zip codes because consumers would not realize that zip codes were personally identifiable).

These recommendations were made by the Electronic Frontier Foundation (EFF) and Hoofnagle.

6. Regulation of Data Providers

Two stakeholders recommended that Companies that provide data to Data Brokers ("Data Providers") should be specifically required to disclose this fact to consumers. The comments further provide that Consumers should be able to opt out/opt in to transfer of data from Data Providers to Data Brokers.

These recommendations were made by Hoofnagle and VPIRG.

7. Credentialing

One comment provided that Data Brokers should be required to screen clients' use of their services and refuse to provide services where the client is engaged in deceptive marketing, stalking, or other illegal behavior.

Data Brokers could give notice of, or share liability, where a client of a Data Broker uses personal information to defraud consumers.

This recommendation was made by Hoofnagle.

8. Respect for Human Rights

One comment recommended that Vermont should make explicit that Data Brokers have a responsibility under the UN Guiding Principles on Business and Human Rights to exercise human rights due diligence to identify, prevent, mitigate and account for the potential human rights risks of their operations. Data Brokers should have systems in place to prevent the company from contributing to human rights abuses.

This recommendation was made by Amnesty International.

9. Government Transparency

One comment recommended that Vermont government agencies that purchase data from data brokers should be transparent about their use of the products, including making contracts publicly available and taking measures to ensure that the data is accurate, and that data, or inferences, about people or groups of people will not lead to discriminatory, or otherwise unlawful outcomes.

This recommendation was made by Amnesty International.

10. Disclosures by Data Broker Customers

One comment recommended that Clients of data brokers should include "how did you get my information" disclosures on direct mail and other personalized advertisements.

This recommendation was made by Hoofnagle.

11. Public Awareness and Education

Two comments recommended that the Attorney General and Department of Financial Regulation should hold a public awareness campaign regarding how consumer information is shared, how consumers can better protect their online privacy, and how 'Do Not Track' browser options work.

This recommendation was made by the ACLU and PrivacyMate.

12. Consumer Protection Act

One comment recommended that the Attorney General should use the Vermont Consumer Protection Statute to prosecute abuses by Data Brokers.

This recommendation was made by the ACLU.

Exhibit B: Massachusetts Data Security Regulation

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

Section:
17.01: Purpose and Scope
17.02: Definitions
17.03: Duty to Protect and Standards for Protecting Personal Information
17.04: Computer System Security Requirements
17.05: Compliance Deadline

17.01: **Purpose and Scope**

(1) Purpose
This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

(2) Scope
The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

17.02: **Definitions**

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

Breach of security, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Electronic, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owns or licenses, receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person, a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

Personal information, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record or Records, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider, any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

17.03: **Duty to Protect and Standards for Protecting Personal Information**

(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and

information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

(a) Designating one or more employees to maintain the comprehensive information security program;

(b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:

1. ongoing employee (including temporary and contract employee) training;
2. employee compliance with policies and procedures; and
3. means for detecting and preventing security system failures.

(c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.

(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

(e) Preventing terminated employees from accessing records containing personal information.

(f) Oversee service providers, by:

1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and
2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 17.03(2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.

(g) Reasonable restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.

(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

(i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

(j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

17.04: **Computer System Security Requirements**

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:
(1) Secure user authentication protocols including:
(a) control of user IDs and other identifiers;
(b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
(c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
(d) restricting access to active users and active user accounts only; and
(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
(2) Secure access control measures that:
(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
(b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
(3)Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
(5) Encryption of all personal information stored on laptops or other portable devices;
(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

17.05: **Compliance Deadline**

(1) Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

REGULATORY AUTHORITY 201 CMR 17.00: M.G.L. c. 93H

Kriger, Ryan

From: Charles Storrow <chuck@leoninepublicaffairs.com>
Sent: Friday, December 15, 2017 1:08 PM
To: Kriger, Ryan; Curtis, Christopher
Subject: RE: Data Broker Working Group

Got it. Thx.

From: Kriger, Ryan [mailto:ryan.kriger@vermont.gov]
Sent: Friday, December 15, 2017 1:08 PM
To: Charles Storrow; Curtis, Christopher
Subject: RE: Data Broker Working Group

Chuck – the report has not yet been released. That "here" is a placeholder. It will be linked before COB.

From: Charles Storrow [mailto:chuck@leoninepublicaffairs.com]
Sent: Friday, December 15, 2017 1:06 PM
To: Curtis, Christopher <Christopher.Curtis@vermont.gov>; Kriger, Ryan <ryan.kriger@vermont.gov>
Subject: FW: Data Broker Working Group

Dear Chris and Ryan,

Below is an email I sent to Ms. Graves in your office, which should be self-explanatory. I got an "out of office" response so I thought I would forward this on to you. Perhaps I am jumping the gun but I get the impression that the report has been released and that it was intended that it be linked on the data broker working group webpage.

Thanks—Chuck

Charles Storrow, Partner
Leonine Public Affairs, LLP
1 Blanchard Court, Suite 101
Montpelier, VT 05602
Cell: (802) 371-7863 – Direct Office: 802-552-4470

chuck@leoninepublicaffairs.com
http://www.leoninepublicaffairs.com/

From: Charles Storrow
Sent: Friday, December 15, 2017 1:03 PM
To: 'my-lanh.graves@vermont.gov'
Subject: Data Broker Working Group

Dear Ms. Graves,

This is to follow up on a voice mail message I just left for you.

The AGO's webpage for the data broker working group indicates that the report due today is available "here," but there is no hyperlink underlying "here."

See: http://ago.vermont.gov/focus/consumer-info/privacy-and-data-security1/data-broker-working-group.php

If that could be fixed and/or if you could email me the report it would be greatly appreciated.

Thanks—Chuck Storrow

Charles Storrow, Partner
Leonine Public Affairs, LLP
1 Blanchard Court, Suite 101
Montpelier, VT 05602
Cell: (802) 371-7863 – Direct Office: 802-552-4470

chuck@leoninepublicaffairs.com
http://www.leoninepublicaffairs.com/

Kriger, Ryan

From: Kriger, Ryan
Sent: Friday, December 15, 2017 1:08 PM
To: Charles Storrow; Curtis, Christopher
Subject: RE: Data Broker Working Group

Chuck – the report has not yet been released. That "here" is a placeholder. It will be linked before COB.

From: Charles Storrow [mailto:chuck@leoninepublicaffairs.com]
Sent: Friday, December 15, 2017 1:06 PM
To: Curtis, Christopher <Christopher.Curtis@vermont.gov>; Kriger, Ryan <ryan.kriger@vermont.gov>
Subject: FW: Data Broker Working Group

Dear Chris and Ryan,

Below is an email I sent to Ms. Graves in your office, which should be self-explanatory. I got an "out of office" response so I thought I would forward this on to you. Perhaps I am jumping the gun but I get the impression that the report has been released and that it was intended that it be linked on the data broker working group webpage.

Thanks—Chuck

Charles Storrow, Partner
Leonine Public Affairs, LLP
1 Blanchard Court, Suite 101
Montpelier, VT 05602
Cell: (802) 371-7863 – Direct Office: 802-552-4470

chuck@leoninepublicaffairs.com
http://www.leoninepublicaffairs.com/

From: Charles Storrow
Sent: Friday, December 15, 2017 1:03 PM
To: 'my-lanh.graves@vermont.gov'
Subject: Data Broker Working Group

Dear Ms. Graves,

This is to follow up on a voice mail message I just left for you.

The AGO's webpage for the data broker working group indicates that the report due today is available "here," but there is no hyperlink underlying "here."

See: http://ago.vermont.gov/focus/consumer-info/privacy-and-data-security1/data-broker-working-group.php

If that could be fixed and/or if you could email me the report it would be greatly appreciated.

Thanks—Chuck Storrow

Charles Storrow, Partner
Leonine Public Affairs, LLP
1 Blanchard Court, Suite 101
Montpelier, VT 05602
Cell: (802) 371-7863 – Direct Office: 802-552-4470

chuck@leoninepublicaffairs.com
http://www.leoninepublicaffairs.com/

Kriger, Ryan

From: Charles Storrow <chuck@leoninepublicaffairs.com>
Sent: Friday, December 15, 2017 1:06 PM
To: Curtis, Christopher; Kriger, Ryan
Subject: FW: Data Broker Working Group

Dear Chris and Ryan,

Below is an email I sent to Ms. Graves in your office, which should be self-explanatory. I got an "out of office" response so I thought I would forward this on to you. Perhaps I am jumping the gun but I get the impression that the report has been released and that it was intended that it be linked on the data broker working group webpage.

Thanks—Chuck

Charles Storrow, Partner
Leonine Public Affairs, LLP
1 Blanchard Court, Suite 101
Montpelier, VT 05602
Cell: (802) 371-7863 – Direct Office: 802-552-4470

chuck@leoninepublicaffairs.com
http://www.leoninepublicaffairs.com/

LEONINE
PUBLIC AFFAIRS

From: Charles Storrow
Sent: Friday, December 15, 2017 1:03 PM
To: 'my-lanh.graves@vermont.gov'
Subject: Data Broker Working Group

Dear Ms. Graves,

This is to follow up on a voice mail message I just left for you.

The AGO's webpage for the data broker working group indicates that the report due today is available "here," but there is no hyperlink underlying "here."

See: http://ago.vermont.gov/focus/consumer-info/privacy-and-data-security1/data-broker-working-group.php

If that could be fixed and/or if you could email me the report it would be greatly appreciated.

Thanks—Chuck Storrow

Charles Storrow, Partner
Leonine Public Affairs, LLP
1 Blanchard Court, Suite 101
Montpelier, VT 05602
Cell: (802) 371-7863 – Direct Office: 802-552-4470

chuck@leoninepublicaffairs.com
http://www.leoninepublicaffairs.com/

Kriger, Ryan

From: Charles Storrow <chuck@leoninepublicaffairs.com>
Sent: Tuesday, December 12, 2017 10:07 AM
To: Curtis, Christopher; Kriger, Ryan
Subject: Data Brokers Report

Dear Chris and Ryan,

When the data broker report comes out it would be greatly appreciated if it could be emailed to me.

Thanks—Chuck Storrow

Charles Storrow, Partner
Leonine Public Affairs, LLP
1 Blanchard Court, Suite 101
Montpelier, VT 05602
Cell: (802) 371-7863 – Direct Office: 802-552-4470

chuck@leoninepublicaffairs.com
http://www.leoninepublicaffairs.com/

Clark, Charity

From: Maggie Lenz <maggie@leoninepublicaffairs.com>
Sent: Tuesday, May 7, 2019 4:23 PM
To: Michael Marcotte
Cc: Kriger, Ryan; David Hall; Clark, Charity
Subject: Re: New S.110 Health Information Language

Yes, we are in agreement. Thank you so much to all parties involved.

Sent from my iPhone

On May 7, 2019, at 4:17 PM, Michael Marcotte <MMarcotte@leg.state.vt.us> wrote:

> Thanks Ryan
>
> Sent from my iPad
>
> On May 7, 2019, at 4:14 PM, Kriger, Ryan <ryan.kriger@vermont.gov> wrote:
>
> > Chairman Marcotte,
> >
> > After much discussion, the following language was arrived at with the State Privacy & Security Coalition. I believe that Facebook was part of these conversations, I'll leave it to Maggie to confirm that her client also agrees with this language.
> >
> > New 9 VSA 2430(10)(vii) (replacing the existing section):
> >
> > (vii) (I) Health, wellness, or fitness records;
> > (II) a health care professional's medical diagnosis or treatment of the consumer; or
> > (III) a health insurance policy number.
> >
> > -Ryan
> >
> > **Ryan G. Kriger**
> > Assistant Attorney General
> > Vermont Office of the Attorney General
> > Public Protection Division
> > 109 State Street
> > Montpelier, VT 05609-1001
> > ph: (802) 828-3170
> > ryan.kriger@vermont.gov

Clark, Charity

From: Maggie Lenz <maggie@leoninepublicaffairs.com>
Sent: Tuesday, October 8, 2019 12:40 PM
To: Kriger, Ryan; Clark, Charity
Cc: Sudbay, William
Subject: Update

Hi there,

TJ asked me to follow up with you after your meeting yesterday re: 2020 legislative priorities. I'm hoping we can hop on a quick call this week if you have time to discuss this, otherwise I'm happy to chat via email if that's easier.

I hope everyone is having a good summer!

Best,

Maggie

Maggie Lenz
Leonine Public Affairs
802.279.4262 (c) 802.229.4900 x. 126 (o)
leoninepublicaffairs.com

Clark, Charity

From: Clark, Charity
Sent: Tuesday, October 8, 2019 3:41 PM
To: Maggie Lenz
Subject: RE: Question

Yes, give him a ring! Jamie's direct dial is 828-5947.
Charity

From: Maggie Lenz <maggie@leoninepublicaffairs.com>
Sent: Tuesday, October 8, 2019 3:32 PM
To: Clark, Charity <Charity.Clark@vermont.gov>
Subject: Re: Question

Thank you!

So in our (FB) meeting with TJ, he brought this initiative up as an example of something FB might be able to help with in state. Is that something I should speak with Jamie about?

Thank you!

Maggie

Maggie Lenz
Leonine Public Affairs
802.279.4262 (c) 802.229.4900 x. 126 (o)
leoninepublicaffairs.com

On Oct 8, 2019, at 3:27 PM, Clark, Charity <Charity.Clark@vermont.gov> wrote:

> Hi, Maggie,
>
> For legislative stuff, it is yours truly. Otherwise, Assistant AG Jamie Renner heads up the EPI. He's great and very knowledgeable.
>
> Charity
>
> **From:** Maggie Lenz <maggie@leoninepublicaffairs.com>
> **Sent:** Tuesday, October 8, 2019 12:43 PM
> **To:** Clark, Charity <Charity.Clark@vermont.gov>
> **Subject:** Question
>
> Hi Charity,
>
> Who is in the point person for the Elder Protection Initiative?
>
> Thanks!!
> Maggie

Maggie Lenz
Leonine Public Affairs
802.279.4262 (c) 802.229.4900 x. 126 (o)
leoninepublicaffairs.com

Clark, Charity

From: Kia Floyd <floydkd@fb.com>
Sent: Wednesday, May 8, 2019 9:23 PM
To: Halpert, Jim
Cc: Kriger, Ryan; teachouts@bcbsvt.com; durkinm@bcbsvt.com; Kingman, Andrew; Maggie Lenz; Clark, Charity
Subject: Re: Wellness Program Definition

We concur. Ryan— We sincerely appreciate your time and effort addressing stakeholders' concerns. We'd like to see the bill move forward tomorrow.

Kia D. Floyd
Facebook Public Policy
d: (202) 368-7469
e: FloydKD@fb.com

Please excuse any typographical errors in my communications. Autotext doesn't like me. 😊

Sent from my iPhone

On May 8, 2019, at 4:49 PM, Halpert, Jim <jim.halpert@dlapiper.com> wrote:

> The State Privacy and Security Coalition is fine with it. BCBS?
>
> **From:** Kriger, Ryan <ryan.kriger@vermont.gov>
> **Sent:** Wednesday, May 08, 2019 4:47 PM
> **To:** teachouts@bcbsvt.com; durkinm@bcbsvt.com; floydkd@fb.com; Kingman, Andrew <andrew.kingman@us.dlapiper.com>; Halpert, Jim <jim.halpert@us.dlapiper.com>; Maggie Lenz <maggie@leoninepublicaffairs.com>; Clark, Charity <Charity.Clark@vermont.gov>
> **Subject:** RE: Wellness Program Definition
>
> **[EXTERNAL]**
>
> ---
>
> I have not received the citation we discussed. I have to leave for the day. I am going to inform leg counsel that there is still dispute over this definition, and recommend a course of action that will allow the committee to vote this out tomorrow.
>
> -Ryan
>
> **Ryan G. Kriger**
> Assistant Attorney General
> Vermont Office of the Attorney General
> Public Protection Division
> 109 State Street
> Montpelier, VT 05609-1001
> ph: (802) 828-3170
> ryan.kriger@vermont.gov

From: Kriger, Ryan
Sent: Wednesday, May 8, 2019 2:10 PM
To: teachouts@bcbsvt.com; durkinm@bcbsvt.com; floydkd@fb.com; andrew.kingman@dlapiper.com; Jim Halpert (jim.halpert@dlapiper.com) <jim.halpert@dlapiper.com>; Maggie Lenz <maggie@leoninepublicaffairs.com>; Clark, Charity <Charity.Clark@vermont.gov>
Subject: Wellness Program Definition

"A wellness program is a program of health promotion or disease prevention." Are we all ok with this definition? It can be found in 45 CFR 146.121 but I'm not sure that's the best cite to use.

If this works, how about something like:

(vii) (I) Health~~, wellness, or fitness~~ records or records of a program of health promotion or disease prevention (wellness program);
(II) a health care professional's medical diagnosis or treatment of the consumer; or
(III) a health insurance policy number.

David Hall might want to tweak this but it gets where I think we need to be. I'd just like to get this out the door to give leg counsel time to make changes.

-Ryan

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

Text exchange between Maggie Lenz and Charity Clark

May 16, 2019, 1:50 PM

ML: Any word yet on meeting?
I am finish errands and coming back soon worried I'm missing it. Ugh I hate this time of year.

CC: Just getting off a call, then back to my parking meter. 🙄 Then, the State House! I'll text you if I hear anything when I get there.

ML: Thank you! I'll do the same if I hear anything.

CC: Rep. Kimball said tomorrow, he's not sure what time, but likely 9 am.

ML: Thank you so much!

May 20, 2019, 3:21 PM

ML: Hiya! So sorry to bug you but if you have any time today would you mind giving me a call?

July 18, 2019, 2:29 PM

ML: Hi Charity, I hope you're having a wonderful summer! I'm wondering if T.J. is going to be around toward the end of September? I'm trying to arrange meetings for Kia Floyd (Facebook) and I'm hoping we could set one up with the AG. I am happy to contact his scheduler (is it Will?) but I lost his contact info. Thank you!

July 19, 2019, 9:59 AM

CC: Hi Maggie! I hope you're having a great, summer, too. I'll text you Will's contact info so you can contact him directly. I will also mention this to T.J.

[Contact Card for Will Sudbay]

ML: Thank you so much!

May 7, 2018

By Electronic Mail

National Association of Attorneys General
1850 M Street, NW
Twelfth Floor
Washington, DC 20036

Re: Facebook Response to National Association of Attorneys General (NAAG)

Dear Attorneys General:

I am writing on behalf of Facebook, Inc. ("Facebook") in response to your March 26, 2018 letter requesting information about the events that have been the focus of recent media attention.

As an initial matter, we take the privacy of our users seriously and strive to be transparent about how Facebook and our applications platform (the "Platform") operate and to inform our users not only how their data may be shared, but also how they can control the types of data that they share publicly, with friends, and with apps. We have been working hard to understand the historical facts relevant to this matter and what we can do to better limit this type of data misuse while continuing to enable third-party experiences on our Platform. Our priority is to assure users that the trust they place in Facebook is deserved and user data is protected on the Platform.

I write now with some information about: (i) Facebook's policies and practices regarding users' data; (ii) the Facebook Platform and the facts related to the misuse of Facebook user data obtained by Dr. Aleksandr Kogan and his company, Global Science Research Ltd. ("GSR") through the "thisisyourdigitallife" application ("the App"); and (iii) the steps that Facebook is taking to address and prevent this type of incident from reoccurring. I hope this letter answers your questions about the events associated with Dr. Kogan, his app, and his improper transfer of information obtained through use of the Platform to SCL Elections Ltd./Cambridge Analytica. As you can imagine, our review is ongoing and this letter represents the Company's current understanding of the relevant issues. Updates will be published to our Newsroom as our review progresses.[1]

We understand the concerns stated in your recent letter and the priority you place on protecting user privacy, and the ability of users to easily control the privacy of their accounts. As our CEO announced, we have taken a number of important steps and

[1] *E.g.*, Facebook Newsroom, *It's Time to Make Our Privacy Tools Easier to Find* (Mar. 28, 2018), https://newsroom.fb.com/news/2018/03/privacy-shortcuts/; Facebook Newsroom, *An Update on Our Plan to Restrict Data Access on Facebook* (Apr. 4, 2018), https://newsroom.fb.com/news/2018/04/restricting-data-access/.

Address: 1 Hacker Way
Menlo Park, CA 94025

made commitments to address data privacy concerns, including: investigating apps on our Platform prior to our privacy restrictions announced in April 2014 that had access to large amounts of data; auditing any app where we identify suspicious activity; telling people affected by apps that have misused their data; turning off apps that the user has not used within the last three months; changing Facebook Login to reduce the data an app can request without App Review; encouraging users to manage the apps they use and making the setting easier to find and manage; and rewarding people who report to us if they find misuses of data by app developers. We believe these steps are directly responsive to the concerns you have identified.

I. Facebook Policies

A. Facebook Privacy Settings and Notice to Users About Sharing Information with Apps

Facebook takes the privacy of its users seriously and enables users of its service to exercise control over the types of data that will be shared publicly, with friends, and with apps. Users can adjust their privacy settings at any time through the Facebook Settings page and can view and adjust some of the most used privacy settings and tools directly from the privacy shortcuts at the top right of any Facebook page. Users can manage their privacy settings to control who can view their profile, posts, and messages, as well as to control their installed apps.

Facebook likewise strives to be transparent with its users about how its Platform operates and to inform its users about the choices they can make with respect to how they can control the information that they share on the Platform. Users are informed of their ability to exercise control over their data in a variety of ways.

1. *Facebook Statement of Rights and Responsibilities ("SRR")*

Facebook's Statement of Rights and Responsibilities is its Terms of Service that governs the relationship between users and others who interact with Facebook, as well as Facebook brands, products and services. Facebook's SRR during the period the App launched and operated on the Platform, to which all users expressly agreed when registering for service, specified that the user owned all the content and information that he or she posted on Facebook, and "can control how it is shared though [their] privacy and application settings."[2] Additionally, the SRR stated that when a user authorized an application, the app may ask for the user's permission to access the user's content and information. The SRR also stated that an app could ask permission to access content and information that others share with the user. Further, the SRR made clear that Facebook required applications to respect the user's privacy, and that the agreement between the user and the app would control how the application can use,

[2] Ex. A, Facebook Statements of Rights and Responsibilities (last revised Jan. 30, 2015, Nov. 15, 2013, and Dec. 11, 2012).

Address: 1 Hacker Way
Menlo Park, CA 94025

store, and transfer that content and information.[3] Facebook's current Terms of Service are available at https://www.facebook.com/terms. The Terms of Service are currently being updated, and the updated Terms of Service can be viewed at https://www.facebook.com/legal/terms/update.

2. *Facebook Data Policy*

The Facebook Data Policy, which all users must confirm that they have read and consent to when registering for service, also explains that users have control regarding whether and to what extent information about them is shared with apps that they may install from the Platform and, prior to May 2015, with apps that their friends may have installed from the Platform.[4] In November 2013, when Dr. Kogan launched the App on Facebook, the Data Policy (then referred to as the Data Use Policy) stated:

> *About Facebook Platform:* Facebook Platform (or simply Platform) refers to the way we help you share your information with the games, applications, and websites you and your friends use. Facebook Platform also lets you bring your friends with you, so you can connect with them off Facebook. In these two ways, Facebook Platform helps you make your experiences on the web more personalized and social.
>
> Remember that these games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook, so you should always make sure to read their terms of service and privacy policies to understand how they treat your data.
>
> *Controlling what information you share with applications*: When you connect with a game, application or website . . . we give the game application, or website (sometimes referred to as just "applications" or "apps") your basic info (we sometimes call this your "public profile"), which includes your User ID and your public information. We also give them your friends' User IDs (also called your friends list) as a part of your basic info.
>
> Your friend list helps the application make your experience more social because it lets you find your friends on that application. Your User ID helps the application personalize

[3] *Id*.
[4] *See* Ex. B, Facebook Data Use Policy (last revised Nov. 15, 2013 and Dec. 11, 2012); Ex. C, Facebook Data Policy (last revised Jan. 30, 2015).

Address: 1 Hacker Way
Menlo Park, CA 94025

> your experience because it can connect your account on that application with your Facebook account, and it can access your basic info, which includes your public information and friend list. This includes the information you choose to make public, as well as information that is always publicly available. If the application needs additional information, such as your stories, photos, or likes, it will have to ask you for specific permission.
>
> The 'Apps' setting lets you control the application you use. You can see the permissions you have given these applications, the last time an application accessed your information, and the audience on Facebook for timeline stories and activity the application posts on your behalf. You can also remove applications you no longer want, or turn off all Platform applications . . . .
>
> *Controlling what is shared when the people you share with use applications*: Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use. . . . If you have made that information public, then the application can access it just like anyone else. But if you've shared your likes with just your friends, the application could ask your friend for permission to share them.
>
> You can control most of the information other people can share with applications they use from the "App" settings page.[5]

The Data Policy was later updated, in January 2015, mid-way through the App's life on the Platform. This updated Data Policy provided users with easy to follow links including: (i) "What kinds of information do we collect?"; (ii) "How do we use this information?"; (iii) "How is this information shared?"; and (iv) "How can I manage or delete information about me?".[6] It further stated that "[w]hen you share and communicate using our Services, you choose the audience who can see what you share" and that "people you share and communicate with may download or re-share this

[5] Ex. B, Facebook Data Use Policy (last revised Nov. 15, 2013 and Dec. 11, 2012).
[6] Ex. C, Facebook Data Policy (last revised Jan. 30, 2015).

content with others on and off our Services."[7] Regarding apps, websites and third-party integrations on or using Facebook services, the updated Data Policy stated:

> When you use third-party apps, websites or other services that use, or are integrated with, our Services, they may receive information about what you post or share. For example, when you play a game with your Facebook friends or use the Facebook Comment or Share button on a website, the game developer or website may get information about your activities in the game or receive a comment or link that you share from their website on Facebook. In addition, when you download or use such third-party services, they can access your Public Profile, which includes your username or user ID, your age range and country/language, your list of friends, as well as any information that you share with them. Information collected by these apps, websites or integrated services is subject to their own terms and policies.
>
> Learn more about how you can control the information about you that you or others share with these apps and websites.[8]

Additionally, the updated Data Policy also provided a link to "Privacy Basics," which gave users the tools to manage and customize their privacy settings, explore ways to increase their account security, as well as provide answers to frequently asked questions about privacy on the Platform.[9] Facebook is currently revising its Data Policy, as described at: https://www.facebook.com/about/privacy/update.

B. Platform Policy

Facebook's Platform Policy also communicates to app developers the relevant requirements regarding users' privacy that apply to apps operating on the Platform, including the requirements to give users choice and control, and to respect user privacy.[10] Application developers explicitly agree to Facebook's Statement of Rights and Responsibilities and Platform Policy when they set up their Facebook accounts. The Platform Policy imposes a variety of obligations on app developers regarding the features, functionality, data collection and usage, and content for apps on the Platform,

[7] *Id*.
[8] *Id*.
[9] *Id*., Facebook Privacy Basics, https://www.facebook.com/about/basics.
[10] Ex. D, Facebook Platform Policy (last revised Mar. 14, 2018), https://developers.facebook.com/policy.

Address: 1 Hacker Way
Menlo Park, CA 94025

as well as Facebook's right to take enforcement action if an application violates the Platform Policy.[11]

Among other things, the Facebook Platform Policy, during the period the App launched and operated on the Platform,[12] included provisions to the following effect:

- Give People Control: Section 2(8): Delete all of a person's data you have received from us (including friend data) if that person asks you to . . . .
- Protect Data: Section 3(3): Only use friend data (including friends list) in the person's experience in your app.
- Protect Data: Section 3(10): Don't transfer any data you receive from us (including anonymous, aggregate, or derived data) to any ad network, data broker or other advertising or monetization-related service.
- Login: Section 7(4): Request only the data and publishing permission your app needs.[13]

The Platform Policy also outlined the actions Facebook could take for violations of the policy:

- Things You Should Know: Section 6(8): We can audit your app to ensure it is safe and does not violate our terms. If requested, you must provide us with proof that your app complies with our terms.[14]
- Things You Should Know: Section 6(15): We may enforce against your app or web site if we conclude that your app violated our terms or is negatively impacting the Platform. We may or may not notify you in advance.[15]
- Things You Should Know: Section 6(16): Enforcement is both automated and manual, and can include disabling your app, restricting you and your app's access to Platform functionality, requiring that you delete data, terminating agreements with you or any other action we deem appropriate.

[11] *Id*.
[12] Ex. E, Facebook Platform Policy (last revised Mar. 25, 2015, Nov. 5, 2014, Aug. 8, 2014, July 24, 2014, and Aug. 20, 2013). Facebook's Platform Policy was restructured and revised in July 2014. The relevant provisions for the purposes of this letter remain substantively the same between the current version and the versions in force during the period the App operated on the Platform.
[13] *See, e.g.*, Ex. E, Facebook Platform Policy (last revised July 24, 2014).
[14] Section 6(8) of the Facebook Platform Policy was added as part of the July 2014 restructuring and revision of the policy.
[15] As part of the July 2014 revision to the Platform Policy, Section 6(15) was clarified to also include enforcement for apps that negatively impacted the Platform.

Address: 1 Hacker Way
Menlo Park, CA 94025

II. Background on Facebook's API Platform and Changes to It

During the time the App was launched and operated on the Platform and through today, Facebook's policies regarding third-party usage of its Platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service.[16]

In November 2013, when Dr. Kogan launched the App, apps generally could be launched on the Platform without affirmative review or approval by Facebook. In April 2014, Facebook announced changes to its Platform that changed apps' ability to request access to data from users. In connection with the transition from the then-existing Platform for app developers (known as "Graph API V1" or "V1") to a new version ("Graph API V2" or "V2"), Facebook enhanced its granular data permissions ("GDP") user interface to give users the ability to pick and choose whether to grant access to each type of data a particular app was requesting (aside from the user's public profile information).[17] V2 also limited the data that apps on the new Platform could access about users' friends. Specifically, after the migration to V2, apps could access only the installing user's public profile, email address, and list of friends who had installed and authorized the same app. All new apps (those launched on Facebook after April 2014) were immediately subject to these new access limitations. For pre-existing apps, there was a one-year grace period (until May 2015) before they were forced to migrate to the V2 Platform and subject to these new limitations. Due to these changes, had Dr. Kogan launched his App on the Platform today, he would not be able to get access to the level of information about users and their friends that he obtained in 2013.

Relatedly, in April 2014 Facebook introduced an "App Review" process requiring Facebook's review and approval before any app could seek permission to access more than certain basic types of an installing user's Facebook data—specifically, any data beyond the user's public profile, email address, and list of friends who also used the app.[18] This App Review process requires developers who create an app that asks for more than this basic user information to justify the data they are looking to collect and how they are going to use it to create a legitimate app experience for users. Only if approved following such review can the app ask for a user's permission to get those data types. Facebook has rejected more than half of the apps submitted for App Review between April 2014 and April 2018.

---

[16] *See* Ex. D, Facebook Platform Policy (last revised Mar. 14, 2018); Ex. E, Facebook Platform Policy (last revised Mar. 25, 2015, Nov. 5, 2014, Aug. 8, 2014, July 24, 2014, and Aug. 20, 2013).
[17] Facebook Newsroom, *Introducing Anonymous Login and an Updated Facebook Login* (Apr. 30, 2014), https://newsroom.fb.com/news/2014/04/f8-introducing-anonymous-login-and-an-updated-facebook-login/.
[18] Jeffrey Spehar, Facebook for Developers, *The New Facebook Login and Graph API 2.0* (Apr. 30, 2014), https://developers.facebook.com/blog/post/2014/04/30/the-new-facebook-login.

Address: 1 Hacker Way
Menlo Park, CA 94025

III. Background on the "thisisyourdigitallife" App and Dr. Kogan

The third-party app "thisisyourdigitallife" was created by Dr. Aleksandr Kogan, a psychology professor and researcher at Cambridge University. The App was launched on the Platform in November 2013.[19] The App was presented to Facebook as a research tool to help Dr. Kogan gather information volunteered by users on Facebook behavior in order to study psychological traits. Our understanding is that the App's appeal to users was that, by being authorized to access their Facebook information, the App would generate and provide users with a personality profile. Dr. Kogan has publicly stated that users were paid a $3-4 reward to install and authorize the App.[20]

During the App's two years of operation on the Platform (from November 2013 to mid-December 2015), approximately 300,000 users (worldwide) installed the App, with about 97% of the installations occurring in the U.S.[21] Like other third-party apps operating on the Platform or on other online platforms at the time, the App asked users for permission to access certain information about or available to those users. Thus, the App obtained access to that information only after the user took affirmative action to install the App and authorize the access.

In November 2013, when Dr. Kogan launched the App, apps generally could be launched on the Platform without affirmative review or approval by Facebook. At that time, the Graph API V1 allowed app developers to request consent to access information entered by the installing user onto his or her Facebook profile—such as name, gender, birthdate, location (i.e., current city or hometown), photos and Page likes—and also (depending on, and in accordance with, each friend's own privacy settings) the same or similar categories of profile information about the user's friends. As explained above in Section II, upon Dr. Kogan's App's forced migration to the V2 Platform, the App could not obtain user data beyond public profile information, email address, and a list of friends who used the App, without clearing Facebook's new App Review process (Kogan tried and failed to clear the new App Review process).

IV. Reports of Data Misuse Trigger Investigation by Facebook Into Allegations

On December 11, 2015, *The Guardian* published an article reporting that Dr. Kogan and his company, GSR, may have passed information the App had obtained from Facebook users to SCL Elections Ltd. ("SCL")/Cambridge Analytica, a firm that does political, governmental, and military work around the globe. By doing so, Dr. Kogan and his company violated Facebook's Platform Policy, which explicitly prohibited selling or licensing user data accessed from Facebook and from sharing any user data accessed

[19] The App was originally named "CPWLab" when it first was placed on the Platform. The name was changed to "GSRApp" on June 11, 2014, and to "thisisyourdigitallife" on July 18, 2014.
[20] BBC Radio 4, Interview with Dr. Aleksandr Kogan at (Mar. 21, 2018), *available at* https://www.bbc.co.uk/programmes/b09vyvxk.
[21] Mark Zuckerberg, Facebook (Mar. 21, 2018), https://www.facebook.com/zuck/posts/10104712037900071.

from Facebook with any ad network, data broker or other advertising or monetization-related service. For this reason, Facebook, on December 17, 2015, banned the App from our Platform and investigated what happened and what further action we should take to enforce our Platform Policy.

In particular, Facebook contacted Dr. Kogan and GSR and demanded that they explain what data they collected, how they used it, and to whom they disclosed it. Facebook further insisted that Dr. Kogan and GSR, as well as other persons or entities to whom they had disclosed any such data, account for and irretrievably delete all such data and information. Facebook also contacted Cambridge Analytica to investigate the allegations reflected in the reporting. Thereafter, Facebook obtained written certifications or confirmations from Dr. Kogan, GSR, and other third parties (including Cambridge Analytica and SCL) declaring that all such data they had obtained was accounted for and destroyed.

Based on information (including the certifications) Facebook obtained after December 11, 2015 as a part of its efforts to investigate the events and enforce its Platform Policy, it was apparent that Dr. Kogan and GSR had shared with Cambridge Analytica data that they had derived from Facebook user information (*i.e.*, predicted personality scores) and potentially some categories of user information directly accessed by the App. This conduct violated Facebook's Platform Policy in the following respects:

- the friends' data the App requested from users was not used solely to augment those users' experience in the App, but apparently had been used independently by GSR to perform its modeling of personality scores;
- GSR appeared to have sold data or data derived from information users had agreed to provide to the App;
- GSR appeared to have transferred to a third-party data or data derived from information users had agreed to provide to the App; and
- the App appeared to have requested permission from users to obtain data that the App itself did not need to function.

In March 2018, Facebook received information from the media suggesting that the certifications we received may not have been accurate and immediately banned SCL Group and Cambridge Analytica from our Platform. Since then, Facebook has been actively investigating the issue, including requesting on-site audits of Cambridge Analytica, Dr. Kogan, and Christopher Wylie.[22] The UK Information Commissioner's Office ("ICO") has asked that Facebook hold off on certain fact-finding steps at this point

[22] Facebook Newsroom, *Pursuing Forensic Audits to Investigate Cambridge Analytica* (Mar. 19, 2018), https://newsroom.fb.com/news/2018/03/forensic-audits-cambridge-analytica/.

Address: 1 Hacker Way
Menlo Park, CA 94025

and Facebook has deferred those actions pending completion of the ICO's investigation. More recently, documents and testimony provided by Mr. Wylie to the UK Parliament (House of Commons Digital, Culture, Media and Sport Committee) suggested that AggregateIQ, a British Columbia-based digital advertising company ("AIQ"), may also have improperly received Facebook user data originally obtained by Dr. Kogan through his App. Facebook has suspended all AIQ accounts of which it is aware on its Platform, pending investigation of what, if any, Facebook user data was obtained by AIQ. Our efforts and our review are ongoing.

To be clear, Dr. Kogan did not access any data to which he was not permitted to access based on the App users' privacy settings and the privacy settings of their friends. Accordingly, there has been no data breach of Facebook's systems. This is not a case of the "thisisyourdigitallife" app, Dr. Kogan/GSR, or SCL/Cambridge Analytica infiltrating Facebook's system or evading data security measures. The information that Dr. Kogan and GSR accessed did not include social security numbers, passwords, or financial or medical data about users.

V. Impact to Users in the United States

We do not know precisely what data Dr. Kogan and GSR shared with Cambridge Analytica and other third parties or exactly how many people were impacted. As described above, Facebook has requested to audit Cambridge Analytica, but that audit request is on hold pending the ICO's investigation. We believe Dr. Kogan and GSR may have improperly shared Facebook information of up to 87 million users with Cambridge Analytica and other third parties. This is our best estimate of the number of users who installed the App plus the number of users who theoretically could have had their data shared with the App due to installations of the App by their friends. We believe that approximately 70 million (or 81%) of these potentially impacted users were located in the United States.[23]

We have compiled State-by-State data regarding installations of the App and State-by-State data regarding what we believe to be the number of users who did not install the App but whose information theoretically could have been shared with the App because they were Facebook friends of people who installed the App and whose privacy settings might have allowed such sharing. Consistent with our intention to be transparent and responsive to the AGs, we provided the State-by-State numbers for distribution to the signatories of the NAAG letter on April 27, 2018. As described in our correspondence, we are still compiling this information for American Samoa and Guam, which we expect to provide in short order.

[23] Facebook Newsroom, *An Update on Our Plan to Restrict Data Access on Facebook* (Apr. 4, 2018), https://newsroom.fb.com/news/2018/04/restricting-data-access/.

VI. What Facebook is Doing Now

Facebook recognizes that, even beyond the changes we have made to our Platform, additional steps can be taken to better protect against potential misuse of information on the Platform. To that end, in recent weeks we have announced a variety of additional measures that we are taking to continue to enhance the Platform. These include investigating apps that had access to large amounts of information before we made the changes to our Platform discussed above, further restricting developers' data access to prevent other potential kinds of abuse, and enhancing users' ability to understand and control their privacy settings and the apps that they interact with on the Platform.[24]

In addition, Facebook has issued notifications to users whose data may have been improperly shared by Dr. Kogan/GSR with Cambridge Analytica or another third party (because either they or their friend installed and authorized the App). Facebook notified users who were potentially impacted by Dr. Kogan's misuse of their data by sharing a link providing details on what categories of their data may have been disclosed.[25] Facebook also displayed a link at the top of users' News Feed to allow users to easily see the apps and websites they used Facebook to log into, and instructions on how users could remove apps they no longer need.[26]

Recently, Facebook's CEO announced a number of additional commitments to address data privacy matters.[27]

- Review our Platform. We will investigate all apps that had access to large amounts of data before we made the 2014 Platform changes described above in more detail, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we will take immediate action, including banning the app from our Platform and pursuing legal action if appropriate.

- Tell people about data misuse. We will tell people affected by apps that have misused their data, to the extent Facebook's current access to historical data allows. This includes building a way for people to know if their data might have been accessed via the App.[28] Moving forward, if we remove an app for misusing data, we will tell everyone who used it.

[24] *Id*.
[25] The user must access his or her Facebook account and News Feed to see the notification.
[26] Mark Zuckerberg, Facebook (Mar. 21, 2018), https://www.facebook.com/zuck/posts/10104712037900071.
[27] *Id.*
[28] Facebook Newsroom, *An Update on Our Plan to Restrict Data Access on Facebook* (Apr. 4, 2018), https://newsroom.fb.com/news/2018/04/restricting-data-access/. As referenced above, Facebook users, who have accessed their accounts, received notifications if they were potentially impacted by Dr. Kogan's misuse of their data.

Address: 1 Hacker Way
Menlo Park, CA 94025

- Turn off access for unused apps. If someone has not used an app within the last three months, we will turn off the app's access to their data.

- Restrict Facebook Login data. We are changing Login, so that in the next version, we will reduce the data that an app can request without App Review to include only name, profile photo and email address. Requesting any other data will require approval from Facebook. Of course, users will retain control over what data any given app can access from their profiles as is true today.

- Encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. Going forward, we're going to make these settings easier to find and manage.

- Reward people who find vulnerabilities. We have also expanded Facebook's bug bounty program so that people can report to us if they find misuse of data by app developers.[29]

In addition, on March 28, 2018, we announced additional changes that the Company will be making with regard to privacy and data protection, including new tools to enhance transparency and control over data for people who use Facebook. Further details of those changes are available at https://newsroom.fb.com/news/2018/03/privacy-shortcuts/.

On April 4, 2018, we provided updates and details on the Company's nine most important changes to protect users' Facebook information. Among other things, as referenced above, starting on April 9, 2018, Facebook began providing users with a link at the top of their News Feed so that they can see what apps they have authorized—and the types of information they have shared with those apps. Users are also able to remove apps that they no longer want.

[29] Facebook Newsroom, *Data Abuse Bounty: Facebook Now Rewards for Reports of Data Abuse* (Apr. 10, 2018), https://newsroom.fb.com/news/2018/04/data-abuse-bounty/.

Thank you for your questions and providing us an opportunity to respond. We are committed to protecting consumers and ensuring that our users' data is not misused by the apps operating on our Platform.

Sincerely,

/s/ Will Castleberry

Will Castleberry
Vice President, US State and Local Policy
Facebook, Inc.

EXHIBIT A

This agreement was written in English (US). To the extent any translated version of this agreement conflicts with the English version, the English version controls. Please note that Section 16 contains certain changes to the general terms for users outside the United States.

Date of Last Revision: January 30, 2015

Statement of Rights and Responsibilities

This Statement of Rights and Responsibilities ("Statement," "Terms," or "SRR") derives from the Facebook Principles, and is our terms of service that governs our relationship with users and others who interact with Facebook, as well as Facebook brands, products and services, which we call the "Facebook Services" or "Services". By using or accessing the Facebook Services, you agree to this Statement, as updated from time to time in accordance with Section 13 below. Additionally, you will find resources at the end of this document that help you understand how Facebook works.

Because Facebook provides a wide range of Services, we may ask you to review and accept supplemental terms that apply to your interaction with a specific app, product, or service. To the extent those supplemental terms conflict with this SRR, the supplemental terms associated with the app, product, or service govern with respect to your use of such app, product or service to the extent of the conflict.

1. **Privacy**

   Your privacy is very important to us. We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Policy, and to use it to help you make informed decisions.

2. **Sharing Your Content and Information**

   You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:

   1. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
   2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
   3. When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, including how you can control what information other people may share with applications, read our Data Policy and Platform Page.)
   4. When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).
   5. We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use your feedback or suggestions without any obligation to compensate you for them (just as you have no obligation to offer them).

3. **Safety**

We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to keep Facebook safe, which includes the following commitments by you:

1. You will not post unauthorized commercial communications (such as spam) on Facebook.
2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.
3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
4. You will not upload viruses or other malicious code.
5. You will not solicit login information or access an account belonging to someone else.
6. You will not bully, intimidate, or harass any user.
7. You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
8. You will not develop or operate a third-party application containing alcohol-related, dating or other mature content (including advertisements) without appropriate age-based restrictions.
9. You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.
10. You will not do anything that could disable, overburden, or impair the proper working or appearance of Facebook, such as a denial of service attack or interference with page rendering or other Facebook functionality.
11. You will not facilitate or encourage any violations of this Statement or our policies.

4. Registration and Account Security

Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
2. You will not create more than one personal account.
3. If we disable your account, you will not create another one without our permission.
4. You will not use your personal timeline primarily for your own commercial gain, and will use a Facebook Page for such purposes.
5. You will not use Facebook if you are under 13.
6. You will not use Facebook if you are a convicted sex offender.
7. You will keep your contact information accurate and up-to-date.
8. You will not share your password (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.
9. You will not transfer your account (including any Page or application you administer) to anyone without first getting our written permission.
10. If you select a username or similar identifier for your account or Page, we reserve the right to remove or reclaim it if we believe it is appropriate (such as when a trademark owner complains about a username that does not closely relate to a user's actual name).

5. Protecting Other People's Rights

We respect other people's rights, and expect you to do the same.

1. You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.
2. We can remove any content or information you post on Facebook if we believe that it violates this Statement or our policies.
3. We provide you with tools to help you protect your intellectual property rights. To learn more, visit our How to Report Claims of Intellectual Property Infringement page.
4. If we remove your content for infringing someone else's copyright, and you believe we removed it by mistake, we will provide you with an opportunity to appeal.

5. If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate.
6. You will not use our copyrights or Trademarks or any confusingly similar marks, except as expressly permitted by our Brand Usage Guidelines or with our prior written permission.
7. If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.
8. You will not post anyone's identification documents or sensitive financial information on Facebook.
9. You will not tag users or send email invitations to non-users without their consent. Facebook offers social reporting tools to enable users to provide feedback about tagging.

6. **Mobile and Other Devices**

1. We currently provide our mobile services for free, but please be aware that your carrier's normal rates and fees, such as text messaging and data charges, will still apply.
2. In the event you change or deactivate your mobile telephone number, you will update your account information on Facebook within 48 hours to ensure that your messages are not sent to the person who acquires your old number.
3. You provide consent and all rights necessary to enable users to sync (including through an application) their devices with any information that is visible to them on Facebook.

7. **Payments**

If you make a payment on Facebook, you agree to our Payments Terms unless it is stated that other terms apply.

8. **Special Provisions Applicable to Developers/Operators of Applications and Websites**

If you are a developer or operator of a Platform application or website or if you use Social Plugins, you must comply with the Facebook Platform Policy.

9. **About Advertisements and Other Commercial Content Served or Enhanced by Facebook**

Our goal is to deliver advertising and other commercial or sponsored content that is valuable to our users and advertisers. In order to help us do that, you agree to the following:

1. You give us permission to use your name, profile picture, content, and information in connection with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.
2. We do not give your content or information to advertisers without your consent.
3. You understand that we may not always identify paid services and communications as such.

10. **Special Provisions Applicable to Advertisers**

If you use our self-service advertising creation interfaces for creation, submission and/or delivery of any advertising or other commercial or sponsored activity or content (collectively, the “Self-Serve Ad Interfaces”), you agree to our Self-Serve Ad Terms. In addition, your advertising or other commercial or sponsored activity or content placed on Facebook or our publisher network will comply with our Advertising Guidelines.

11. **Special Provisions Applicable to Pages**

If you create or administer a Page on Facebook, or run a promotion or an offer from your Page, you agree to our Pages Terms.

12. **Special Provisions Applicable to Software**

    1. If you download or use our software, such as a stand-alone software product, an app, or a browser plugin, you agree that from time to time, the software may download and install upgrades, updates and additional features from us in order to improve, enhance, and further develop the software.
    2. You will not modify, create derivative works of, decompile, or otherwise attempt to extract source code from us, unless you are expressly permitted to do so under an open source license, or we give you express written permission.

13. **Amendments**

    1. We'll notify you before we make changes to these terms and give you the opportunity to review and comment on the revised terms before continuing to use our Services.
    2. If we make changes to policies, guidelines or other terms referenced in or incorporated by this Statement, we may provide notice on the Site Governance Page.
    3. Your continued use of the Facebook Services, following notice of the changes to our terms, policies or guidelines, constitutes your acceptance of our amended terms, policies or guidelines.

14. **Termination**

    If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account. You may also delete your account or disable your application at any time. In all such cases, this Statement shall terminate, but the following provisions will still apply: 2.2, 2.4, 3-5, 9.3, and 14-18.

15. **Disputes**

    1. You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such claims. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions.
    2. If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim. Although we provide rules for user conduct, we do not control or direct users' actions on Facebook and are not responsible for the content or information users transmit or share on Facebook. We are not responsible for any offensive, inappropriate, obscene, unlawful or otherwise objectionable content or information you may encounter on Facebook. We are not responsible for the conduct, whether online or offline, of any user of Facebook.
    3. WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK AS IS WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE DO NOT GUARANTEE THAT FACEBOOK WILL ALWAYS BE SAFE, SECURE OR ERROR-FREE OR THAT FACEBOOK WILL ALWAYS FUNCTION WITHOUT DISRUPTIONS, DELAYS OR IMPERFECTIONS. FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT,

INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES. IF YOU ARE A CALIFORNIA RESIDENT, YOU WAIVE CALIFORNIA CIVIL CODE §1542, WHICH SAYS: A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS OR HER FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM OR HER MUST HAVE MATERIALLY AFFECTED HIS OR HER SETTLEMENT WITH THE DEBTOR. WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS ($100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS. APPLICABLE LAW MAY NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN SUCH CASES, FACEBOOK'S LIABILITY WILL BE LIMITED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW.

16. **Special Provisions Applicable to Users Outside the United States**

We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users and non-users who interact with Facebook outside the United States:

1. You consent to having your personal data transferred to and processed in the United States.
2. If you are located in a country embargoed by the United States, or are on the U.S. Treasury Department's list of Specially Designated Nationals you will not engage in commercial activities on Facebook (such as advertising or payments) or operate a Platform application or website. You will not use Facebook if you are prohibited from receiving products, services, or software originating from the United States.
3. Certain specific terms that apply only for German users are available here.

17. **Definitions**

1. By "Facebook" or" Facebook Services" we mean the features and services we make available, including through (a) our website at www.facebook.com and any other Facebook branded or co-branded websites (including sub-domains, international versions, widgets, and mobile versions); (b) our Platform; (c) social plugins such as the Like button, the Share button and other similar offerings; and (d) other media, brands, products, services, software (such as a toolbar), devices, or networks now existing or later developed. Facebook reserves the right to designate, in its sole discretion, that certain of our brands, products, or services are governed by separate terms and not this SRR.
2. By "Platform" we mean a set of APIs and services (such as content) that enable others, including application developers and website operators, to retrieve data from Facebook or provide data to us.
3. By "information" we mean facts and other information about you, including actions taken by users and non-users who interact with Facebook.
4. By "content" we mean anything you or other users post, provide or share using Facebook Services.
5. By "data" or "user data" or "user's data" we mean any data, including a user's content or information that you or third parties can retrieve from Facebook or provide to Facebook through Platform.
6. By "post" we mean post on Facebook or otherwise make available by using Facebook.
7. By "use" we mean use, run, copy, publicly perform or display, distribute, modify, translate, and create derivative works of.
8. By "application" we mean any application or website that uses or accesses Platform, as well as anything else that receives or has received data from us. If you no longer access Platform but have not deleted all data from us, the term application will apply until you delete the data.

9. By “Trademarks” we mean the list of trademarks provided here.

18. **Other**

    1. If you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and Facebook Ireland Limited. References to “us,” “we,” and “our” mean either Facebook, Inc. or Facebook Ireland Limited, as appropriate.
    2. This Statement makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements.
    3. If any portion of this Statement is found to be unenforceable, the remaining portion will remain in full force and effect.
    4. If we fail to enforce any of this Statement, it will not be considered a waiver.
    5. Any amendment to or waiver of this Statement must be made in writing and signed by us.
    6. You will not transfer any of your rights or obligations under this Statement to anyone else without our consent.
    7. All of our rights and obligations under this Statement are freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise.
    8. Nothing in this Statement shall prevent us from complying with the law.
    9. This Statement does not confer any third party beneficiary rights.
    10. We reserve all rights not expressly granted to you.
    11. You will comply with all applicable laws when using or accessing Facebook.

By using or accessing Facebook Services, you agree that we can collect and use such content and information in accordance with the Data Policy as amended from time to time. You may also want to review the following documents, which provide additional information about your use of Facebook:

- Payment Terms: These additional terms apply to all payments made on or through Facebook, unless it is stated that other terms apply.
- Platform Page: This page helps you better understand what happens when you add a third-party application or use Facebook Connect, including how they may access and use your data.
- Facebook Platform Policies: These guidelines outline the policies that apply to applications, including Connect sites.
- Advertising Guidelines: These guidelines outline the policies that apply to advertisements placed on Facebook.
- Self-Serve Ad Terms: These terms apply when you use the Self-Serve Ad Interfaces to create, submit, or deliver any advertising or other commercial or sponsored activity or content.
- Promotions Guidelines: These guidelines outline the policies that apply if you offer contests, sweepstakes, and other types of promotions on Facebook.
- Facebook Brand Resources: These guidelines outline the policies that apply to use of Facebook trademarks, logos and screenshots.
- How to Report Claims of Intellectual Property Infringement
- Pages Terms: These guidelines apply to your use of Facebook Pages.
- Community Standards: These guidelines outline our expectations regarding the content you post to Facebook and your activity on Facebook.

To access the Statement of Rights and Responsibilities in several different languages, change the language setting for your Facebook session by clicking on the language link in the left corner of most pages. If the Statement is not available in the language you select, we will default to the English version.

This agreement was written in English (US). To the extent any translated version of this agreement conflicts with the English version, the English version controls. Please note that Section 17 contains certain changes to the general terms for users outside the United States.

Date of Last Revision: November 15, 2013.

Statement of Rights and Responsibilities

This Statement of Rights and Responsibilities ("Statement," "Terms," or "SRR") derives from the Facebook Principles, and is our terms of service that governs our relationship with users and others who interact with Facebook. By using or accessing Facebook, you agree to this Statement, as updated from time to time in accordance with Section 14 below. Additionally, you will find resources at the end of this document that help you understand how Facebook works.

1. **Privacy**

   Your privacy is very important to us. We designed our Data Use Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Use Policy, and to use it to help you make informed decisions.

2. **Sharing Your Content and Information**

   You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:
   1. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
   2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
   3. When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, including how you can control what information other people may share with applications, read our Data Use Policy and Platform Page.)
   4. When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).
   5. We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use them without any obligation to compensate you for them (just as you have no obligation to offer them).

3. **Safety**

   We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to keep Facebook safe, which includes the following commitments by you:
   1. You will not post unauthorized commercial communications (such as spam) on Facebook.
   2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.

3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
4. You will not upload viruses or other malicious code.
5. You will not solicit login information or access an account belonging to someone else.
6. You will not bully, intimidate, or harass any user.
7. You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
8. You will not develop or operate a third-party application containing alcohol-related, dating or other mature content (including advertisements) without appropriate age-based restrictions.
9. You will follow our Promotions Guidelines and all applicable laws if you publicize or offer any contest, giveaway, or sweepstakes ("promotion") on Facebook.
10. You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.
11. You will not do anything that could disable, overburden, or impair the proper working or appearance of Facebook, such as a denial of service attack or interference with page rendering or other Facebook functionality.
12. You will not facilitate or encourage any violations of this Statement or our policies.

4. **Registration and Account Security**

Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
2. You will not create more than one personal account.
3. If we disable your account, you will not create another one without our permission.
4. You will not use your personal timeline primarily for your own commercial gain, and will use a Facebook Page for such purposes.
5. You will not use Facebook if you are under 13.
6. You will not use Facebook if you are a convicted sex offender.
7. You will keep your contact information accurate and up-to-date.
8. You will not share your password (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.
9. You will not transfer your account (including any Page or application you administer) to anyone without first getting our written permission.
10. If you select a username or similar identifier for your account or Page, we reserve the right to remove or reclaim it if we believe it is appropriate (such as when a trademark owner complains about a username that does not closely relate to a user's actual name).

5. **Protecting Other People's Rights**

We respect other people's rights, and expect you to do the same.

1. You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.
2. We can remove any content or information you post on Facebook if we believe that it violates this Statement or our policies.
3. We provide you with tools to help you protect your intellectual property rights. To learn more, visit our How to Report Claims of Intellectual Property Infringement page.
4. If we remove your content for infringing someone else's copyright, and you believe we removed it by mistake, we will provide you with an opportunity to appeal.
5. If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate.
6. You will not use our copyrights or trademarks (including Facebook, the Facebook and F Logos, FB, Face, Poke, Book and Wall), or any confusingly similar marks, except as expressly permitted by our Brand

Usage Guidelines or with our prior written permission.

7. If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.
8. You will not post anyone's identification documents or sensitive financial information on Facebook.
9. You will not tag users or send email invitations to non-users without their consent. Facebook offers social reporting tools to enable users to provide feedback about tagging.

6. **Mobile and Other Devices**

1. We currently provide our mobile services for free, but please be aware that your carrier's normal rates and fees, such as text messaging and data charges, will still apply.
2. In the event you change or deactivate your mobile telephone number, you will update your account information on Facebook within 48 hours to ensure that your messages are not sent to the person who acquires your old number.
3. You provide consent and all rights necessary to enable users to sync (including through an application) their devices with any information that is visible to them on Facebook.

7. **Payments**

If you make a payment on Facebook or use Facebook Credits, you agree to our Payments Terms.

8. **Special Provisions Applicable to Social Plugins**

If you include our Social Plugins, such as the Share or Like buttons on your website, the following additional terms apply to you:

1. We give you permission to use Facebook's Social Plugins so that users can post links or content from your website on Facebook.
2. You give us permission to use and allow others to use such links and content on Facebook.
3. You will not place a Social Plugin on any page containing content that would violate this Statement if posted on Facebook.

9. **Special Provisions Applicable to Developers/Operators of Applications and Websites**

If you are a developer or operator of a Platform application or website, the following additional terms apply to you:

1. You are responsible for your application and its content and all uses you make of Platform. This includes ensuring your application or use of Platform meets our Facebook Platform Policies and our Advertising Guidelines.
2. Your access to and use of data you receive from Facebook, will be limited as follows:
    1. You will only request data you need to operate your application.
    2. You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data and you will include your privacy policy URL in the Developer Application.
    3. You will not use, display, share, or transfer a user’s data in a manner inconsistent with your privacy policy.
    4. You will delete all data you receive from us concerning a user if the user asks you to do so, and will provide a mechanism for users to make such a request.
    5. You will not include data you receive from us concerning a user in any advertising creative.
    6. You will not directly or indirectly transfer any data you receive from us to (or use such data in

connection with) any ad network, ad exchange, data broker, or other advertising related toolset, even if a user consents to that transfer or use.
    7. You will not sell user data. If you are acquired by or merge with a third party, you can continue to use user data within your application, but you cannot transfer user data outside of your application.
    8. We can require you to delete user data if you use it in a way that we determine is inconsistent with users' expectations.
    9. We can limit your access to data.
    10. You will comply with all other restrictions contained in our Facebook Platform Policies.
3. You will not give us information that you independently collect from a user or a user's content without that user's consent.
4. You will make it easy for users to remove or disconnect from your application.
5. You will make it easy for users to contact you. We can also share your email address with users and others claiming that you have infringed or otherwise violated their rights.
6. You will provide customer support for your application.
7. You will not show third party ads or web search boxes on www.facebook.com.
8. We give you all rights necessary to use the code, APIs, data, and tools you receive from us.
9. You will not sell, transfer, or sublicense our code, APIs, or tools to anyone.
10. You will not misrepresent your relationship with Facebook to others.
11. You may use the logos we make available to developers or issue a press release or other public statement so long as you follow our Facebook Platform Policies.
12. We can issue a press release describing our relationship with you.
13. You will comply with all applicable laws. In particular you will (if applicable):
    1. have a policy for removing infringing content and terminating repeat infringers that complies with the Digital Millennium Copyright Act.
    2. comply with the Video Privacy Protection Act (VPPA), and obtain any opt-in consent necessary from users so that user data subject to the VPPA may be shared on Facebook. You represent that any disclosure to us will not be incidental to the ordinary course of your business.
14. We do not guarantee that Platform will always be free.
15. You give us all rights necessary to enable your application to work with Facebook, including the right to incorporate content and information you provide to us into streams, timelines, and user action stories.
16. You give us the right to link to or frame your application, and place content, including ads, around your application.
17. We can analyze your application, content, and data for any purpose, including commercial (such as for targeting the delivery of advertisements and indexing content for search).
18. To ensure your application is safe for users, we can audit it.
19. We can create applications that offer similar features and services to, or otherwise compete with, your application.

10. About Advertisements and Other Commercial Content Served or Enhanced by Facebook

Our goal is to deliver advertising and other commercial or sponsored content that is valuable to our users and advertisers. In order to help us do that, you agree to the following:

1. You give us permission to use your name, profile picture, content, and information in connection with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.

2. We do not give your content or information to advertisers without your consent.
3. You understand that we may not always identify paid services and communications as such.

11. **Special Provisions Applicable to Advertisers**

You can target your desired audience by buying ads on Facebook or our publisher network. The following additional terms apply to you if you place an order through our online advertising portal (Order):

1. When you place an Order, you will tell us the type of advertising you want to buy, the amount you want to spend, and your bid. If we accept your Order, we will deliver your ads as inventory becomes available. When serving your ad, we do our best to deliver the ads to the audience you specify, although we cannot guarantee in every instance that your ad will reach its intended target.
2. In instances where we believe doing so will enhance the effectiveness of your advertising campaign, we may broaden the targeting criteria you specify.
3. You will pay for your Orders in accordance with our Payments Terms. The amount you owe will be calculated based on our tracking mechanisms.
4. Your ads will comply with our Advertising Guidelines.
5. We will determine the size, placement, and positioning of your ads.
6. We do not guarantee the activity that your ads will receive, such as the number of clicks your ads will get.
7. We cannot control how clicks are generated on your ads. We have systems that attempt to detect and filter certain click activity, but we are not responsible for click fraud, technological issues, or other potentially invalid click activity that may affect the cost of running ads.
8. You can cancel your Order at any time through our online portal, but it may take up to 24 hours before the ad stops running. You are responsible for paying for all ads that run.
9. Our license to run your ad will end when we have completed your Order. You understand, however, that if users have interacted with your ad, your ad may remain until the users delete it.
10. We can use your ads and related content and information for marketing or promotional purposes.
11. You will not issue any press release or make public statements about your relationship with Facebook without our prior written permission.
12. We may reject or remove any ad for any reason.
13. If you are placing ads on someone else's behalf, you must have permission to place those ads, including the following:
    1. You warrant that you have the legal authority to bind the advertiser to this Statement.
    2. You agree that if the advertiser you represent violates this Statement, we may hold you responsible for that violation.

12. **Special Provisions Applicable to Pages**

If you create or administer a Page on Facebook, or run a promotion or an offer from your Page, you agree to our Pages Terms.

13. **Special Provisions Applicable to Software**

1. If you download or use our software, such as a stand-alone software product, an app, or a browser plugin, you agree that from time to time, the software may download and install upgrades, updates and additional features from us in order to improve, enhance, and further develop the software.
2. You will not modify, create derivative works of, decompile, or otherwise attempt to extract source code from us, unless you are expressly permitted to do so under an open source license, or we give you express written permission.

14. **Amendments**

1. Unless we make a change for legal or administrative reasons, or to correct an inaccurate statement, we will provide you with seven (7) days notice (for example, by posting the change on the Facebook Site Governance Page) and an opportunity to comment on changes to this Statement. You can also visit our

Facebook Site Governance Page and "like" the Page to get updates about changes to this Statement.

2. If we make changes to policies referenced in or incorporated by this Statement, we may provide notice on the Site Governance Page.
3. Your continued use of Facebook following changes to our terms constitutes your acceptance of our amended terms.

15. **Termination**

If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account. You may also delete your account or disable your application at any time. In all such cases, this Statement shall terminate, but the following provisions will still apply: 2.2, 2.4, 3-5, 8.2, 9.1-9.3, 9.9, 9.10, 9.13, 9.15, 9.18, 10.3, 11.2, 11.5, 11.6, 11.9, 11.12, 11.13, and 15-19.

16. **Disputes**

1. You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such claims. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions.
2. If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim. Although we provide rules for user conduct, we do not control or direct users' actions on Facebook and are not responsible for the content or information users transmit or share on Facebook. We are not responsible for any offensive, inappropriate, obscene, unlawful or otherwise objectionable content or information you may encounter on Facebook. We are not responsible for the conduct, whether online or offline, or any user of Facebook.
3. WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK AS IS WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE DO NOT GUARANTEE THAT FACEBOOK WILL ALWAYS BE SAFE, SECURE OR ERROR-FREE OR THAT FACEBOOK WILL ALWAYS FUNCTION WITHOUT DISRUPTIONS, DELAYS OR IMPERFECTIONS. FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES. IF YOU ARE A CALIFORNIA RESIDENT, YOU WAIVE CALIFORNIA CIVIL CODE §1542, WHICH SAYS: A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM MUST HAVE MATERIALLY AFFECTED HIS SETTLEMENT WITH THE DEBTOR. WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS ($100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS. APPLICABLE LAW MAY NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN

SUCH CASES, FACEBOOK'S LIABILITY WILL BE LIMITED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW.

17. **Special Provisions Applicable to Users Outside the United States**

We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users and non-users who interact with Facebook outside the United States:

1. You consent to having your personal data transferred to and processed in the United States.
2. If you are located in a country embargoed by the United States, or are on the U.S. Treasury Department's list of Specially Designated Nationals you will not engage in commercial activities on Facebook (such as advertising or payments) or operate a Platform application or website. You will not use Facebook if you are prohibited from receiving products, services, or software originating from the United States.
3. Certain specific terms that apply only for German users are available here.

18. **Definitions**

1. By "Facebook" we mean the features and services we make available, including through (a) our website at www.facebook.com and any other Facebook branded or co-branded websites (including sub-domains, international versions, widgets, and mobile versions); (b) our Platform; (c) social plugins such as the Like button, the Share button and other similar offerings and (d) other media, software (such as a toolbar), devices, or networks now existing or later developed.
2. By "Platform" we mean a set of APIs and services (such as content) that enable others, including application developers and website operators, to retrieve data from Facebook or provide data to us.
3. By "information" we mean facts and other information about you, including actions taken by users and non-users who interact with Facebook.
4. By "content" we mean anything you or other users post on Facebook that would not be included in the definition of information.
5. By "data" or "user data" or "user's data" we mean any data, including a user's content or information that you or third parties can retrieve from Facebook or provide to Facebook through Platform.
6. By "post" we mean post on Facebook or otherwise make available by using Facebook.
7. By "use" we mean use, run, copy, publicly perform or display, distribute, modify, translate, and create derivative works of.
8. By "active registered user" we mean a user who has logged into Facebook at least once in the previous 30 days.
9. By "application" we mean any application or website that uses or accesses Platform, as well as anything else that receives or has received data from us. If you no longer access Platform but have not deleted all data from us, the term application will apply until you delete the data.

19. **Other**

1. If you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and Facebook Ireland Limited. References to “us,” “we,” and “our” mean either Facebook, Inc. or Facebook Ireland Limited, as appropriate.
2. This Statement makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements.
3. If any portion of this Statement is found to be unenforceable, the remaining portion will remain in full force and effect.
4. If we fail to enforce any of this Statement, it will not be considered a waiver.
5. Any amendment to or waiver of this Statement must be made in writing and signed by us.
6. You will not transfer any of your rights or obligations under this Statement to anyone else without our

consent.

7. All of our rights and obligations under this Statement are freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise.
8. Nothing in this Statement shall prevent us from complying with the law.
9. This Statement does not confer any third party beneficiary rights.
10. We reserve all rights not expressly granted to you.
11. You will comply with all applicable laws when using or accessing Facebook.

You may also want to review the following documents, which provide additional information about your use of Facebook:

- Data Use Policy: The Data Use Policy contains information to help you understand how we collect and use information.
- Payment Terms: These additional terms apply to all payments made on or through Facebook.
- Platform Page: This page helps you better understand what happens when you add a third-party application or use Facebook Connect, including how they may access and use your data.
- Facebook Platform Policies: These guidelines outline the policies that apply to applications, including Connect sites.
- Advertising Guidelines: These guidelines outline the policies that apply to advertisements placed on Facebook.
- Promotions Guidelines: These guidelines outline the policies that apply if you offer contests, sweepstakes, and other types of promotions on Facebook.
- Facebook Brand Resources: These guidelines outline the policies that apply to use of Facebook trademarks, logos and screenshots.
- How to Report Claims of Intellectual Property Infringement
- Pages Terms: These guidelines apply to your use of Facebook Pages.
- Community Standards: These guidelines outline our expectations regarding the content you post to Facebook and your activity on Facebook.

To access the Statement of Rights and Responsibilities in several different languages, change the language setting for your Facebook session by clicking on the language link in the left corner of most pages. If the Statement is not available in the language you select, we will default to the English version.

This agreement was written in English (US). To the extent any translated version of this agreement conflicts with the English version, the English version controls. Please note that Section 17 contains certain changes to the general terms for users outside the United States.

Date of Last Revision: December 11, 2012.

Statement of Rights and Responsibilities

This Statement of Rights and Responsibilities ("Statement," "Terms," or "SRR") derives from the Facebook Principles, and is our terms of service that governs our relationship with users and others who interact with Facebook. By using or accessing Facebook, you agree to this Statement, as updated from time to time in accordance with Section 14 below. Additionally, you will find resources at the end of this document that help you understand how Facebook works.

1. **Privacy**

   Your privacy is very important to us. We designed our Data Use Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Use Policy, and to use it to help you make informed decisions.

2. **Sharing Your Content and Information**

   You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:
   1. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
   2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
   3. When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, including how you can control what information other people may share with applications, read our Data Use Policy and Platform Page.)
   4. When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).
   5. We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use them without any obligation to compensate you for them (just as you have no obligation to offer them).

3. **Safety**

   We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to keep Facebook safe, which includes the following commitments by you:
   1. You will not post unauthorized commercial communications (such as spam) on Facebook.
   2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.

3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
4. You will not upload viruses or other malicious code.
5. You will not solicit login information or access an account belonging to someone else.
6. You will not bully, intimidate, or harass any user.
7. You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
8. You will not develop or operate a third-party application containing alcohol-related, dating or other mature content (including advertisements) without appropriate age-based restrictions.
9. You will follow our Promotions Guidelines and all applicable laws if you publicize or offer any contest, giveaway, or sweepstakes ("promotion") on Facebook.
10. You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.
11. You will not do anything that could disable, overburden, or impair the proper working or appearance of Facebook, such as a denial of service attack or interference with page rendering or other Facebook functionality.
12. You will not facilitate or encourage any violations of this Statement or our policies.

4. **Registration and Account Security**

Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
2. You will not create more than one personal account.
3. If we disable your account, you will not create another one without our permission.
4. You will not use your personal timeline primarily for your own commercial gain, and will use a Facebook Page for such purposes.
5. You will not use Facebook if you are under 13.
6. You will not use Facebook if you are a convicted sex offender.
7. You will keep your contact information accurate and up-to-date.
8. You will not share your password (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.
9. You will not transfer your account (including any Page or application you administer) to anyone without first getting our written permission.
10. If you select a username or similar identifier for your account or Page, we reserve the right to remove or reclaim it if we believe it is appropriate (such as when a trademark owner complains about a username that does not closely relate to a user's actual name).

5. **Protecting Other People's Rights**

We respect other people's rights, and expect you to do the same.

1. You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.
2. We can remove any content or information you post on Facebook if we believe that it violates this Statement or our policies.
3. We provide you with tools to help you protect your intellectual property rights. To learn more, visit our How to Report Claims of Intellectual Property Infringement page.
4. If we remove your content for infringing someone else's copyright, and you believe we removed it by mistake, we will provide you with an opportunity to appeal.
5. If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate.
6. You will not use our copyrights or trademarks (including Facebook, the Facebook and F Logos, FB, Face, Poke, Book and Wall), or any confusingly similar marks, except as expressly permitted by our Brand

Usage Guidelines or with our prior written permission.

7. If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.
8. You will not post anyone's identification documents or sensitive financial information on Facebook.
9. You will not tag users or send email invitations to non-users without their consent. Facebook offers social reporting tools to enable users to provide feedback about tagging.

6. **Mobile and Other Devices**

1. We currently provide our mobile services for free, but please be aware that your carrier's normal rates and fees, such as text messaging fees, will still apply.
2. In the event you change or deactivate your mobile telephone number, you will update your account information on Facebook within 48 hours to ensure that your messages are not sent to the person who acquires your old number.
3. You provide consent and all rights necessary to enable users to sync (including through an application) their devices with any information that is visible to them on Facebook.

7. **Payments**

If you make a payment on Facebook or use Facebook Credits, you agree to our Payments Terms.

8. **Special Provisions Applicable to Social Plugins**

If you include our Social Plugins, such as the Share or Like buttons on your website, the following additional terms apply to you:

1. We give you permission to use Facebook's Social Plugins so that users can post links or content from your website on Facebook.
2. You give us permission to use and allow others to use such links and content on Facebook.
3. You will not place a Social Plugin on any page containing content that would violate this Statement if posted on Facebook.

9. **Special Provisions Applicable to Developers/Operators of Applications and Websites**

If you are a developer or operator of a Platform application or website, the following additional terms apply to you:

1. You are responsible for your application and its content and all uses you make of Platform. This includes ensuring your application or use of Platform meets our Facebook Platform Policies and our Advertising Guidelines.
2. Your access to and use of data you receive from Facebook, will be limited as follows:
    1. You will only request data you need to operate your application.
    2. You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data and you will include your privacy policy URL in the Developer Application.
    3. You will not use, display, share, or transfer a user’s data in a manner inconsistent with your privacy policy.
    4. You will delete all data you receive from us concerning a user if the user asks you to do so, and will provide a mechanism for users to make such a request.
    5. You will not include data you receive from us concerning a user in any advertising creative.
    6. You will not directly or indirectly transfer any data you receive from us to (or use such data in

connection with) any ad network, ad exchange, data broker, or other advertising related toolset, even if a user consents to that transfer or use.
    7. You will not sell user data. If you are acquired by or merge with a third party, you can continue to use user data within your application, but you cannot transfer user data outside of your application.
    8. We can require you to delete user data if you use it in a way that we determine is inconsistent with users' expectations.
    9. We can limit your access to data.
    10. You will comply with all other restrictions contained in our Facebook Platform Policies.
3. You will not give us information that you independently collect from a user or a user's content without that user's consent.
4. You will make it easy for users to remove or disconnect from your application.
5. You will make it easy for users to contact you. We can also share your email address with users and others claiming that you have infringed or otherwise violated their rights.
6. You will provide customer support for your application.
7. You will not show third party ads or web search boxes on www.facebook.com.
8. We give you all rights necessary to use the code, APIs, data, and tools you receive from us.
9. You will not sell, transfer, or sublicense our code, APIs, or tools to anyone.
10. You will not misrepresent your relationship with Facebook to others.
11. You may use the logos we make available to developers or issue a press release or other public statement so long as you follow our Facebook Platform Policies.
12. We can issue a press release describing our relationship with you.
13. You will comply with all applicable laws. In particular you will (if applicable):
    1. have a policy for removing infringing content and terminating repeat infringers that complies with the Digital Millennium Copyright Act.
    2. comply with the Video Privacy Protection Act (VPPA), and obtain any opt-in consent necessary from users so that user data subject to the VPPA may be shared on Facebook. You represent that any disclosure to us will not be incidental to the ordinary course of your business.
14. We do not guarantee that Platform will always be free.
15. You give us all rights necessary to enable your application to work with Facebook, including the right to incorporate content and information you provide to us into streams, timelines, and user action stories.
16. You give us the right to link to or frame your application, and place content, including ads, around your application.
17. We can analyze your application, content, and data for any purpose, including commercial (such as for targeting the delivery of advertisements and indexing content for search).
18. To ensure your application is safe for users, we can audit it.
19. We can create applications that offer similar features and services to, or otherwise compete with, your application.

10. About Advertisements and Other Commercial Content Served or Enhanced by Facebook

Our goal is to deliver ads and commercial content that are valuable to our users and advertisers. In order to help us do that, you agree to the following:

1. You can use your privacy settings to limit how your name and profile picture may be associated with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. You give us permission to use your name and profile picture in connection with that content, subject to the limits you place.
2. We do not give your content or information to advertisers without your consent.
3. You understand that we may not always identify paid services and communications as such.

11. Special Provisions Applicable to Advertisers

You can target your desired audience by buying ads on Facebook or our publisher network. The following

additional terms apply to you if you place an order through our online advertising portal (Order):

1. When you place an Order, you will tell us the type of advertising you want to buy, the amount you want to spend, and your bid. If we accept your Order, we will deliver your ads as inventory becomes available. When serving your ad, we do our best to deliver the ads to the audience you specify, although we cannot guarantee in every instance that your ad will reach its intended target.
2. In instances where we believe doing so will enhance the effectiveness of your advertising campaign, we may broaden the targeting criteria you specify.
3. You will pay for your Orders in accordance with our Payments Terms. The amount you owe will be calculated based on our tracking mechanisms.
4. Your ads will comply with our Advertising Guidelines.
5. We will determine the size, placement, and positioning of your ads.
6. We do not guarantee the activity that your ads will receive, such as the number of clicks your ads will get.
7. We cannot control how clicks are generated on your ads. We have systems that attempt to detect and filter certain click activity, but we are not responsible for click fraud, technological issues, or other potentially invalid click activity that may affect the cost of running ads.
8. You can cancel your Order at any time through our online portal, but it may take up to 24 hours before the ad stops running. You are responsible for paying for all ads that run.
9. Our license to run your ad will end when we have completed your Order. You understand, however, that if users have interacted with your ad, your ad may remain until the users delete it.
10. We can use your ads and related content and information for marketing or promotional purposes.
11. You will not issue any press release or make public statements about your relationship with Facebook without our prior written permission.
12. We may reject or remove any ad for any reason.
13. If you are placing ads on someone else's behalf, you must have permission to place those ads, including the following:
    1. You warrant that you have the legal authority to bind the advertiser to this Statement.
    2. You agree that if the advertiser you represent violates this Statement, we may hold you responsible for that violation.

12. Special Provisions Applicable to Pages

If you create or administer a Page on Facebook, or run a promotion or an offer from your Page, you agree to our Pages Terms.

13. Special Provisions Applicable to Software

1. If you download our software, such as a stand-alone software product or a browser plugin, you agree that from time to time, the software may download upgrades, updates and additional features from us in order to improve, enhance and further develop the software.
2. You will not modify, create derivative works of, decompile or otherwise attempt to extract source code from us, unless you are expressly permitted to do so under an open source license or we give you express written permission.

14. Amendments

1. Unless we make a change for legal or administrative reasons, or to correct an inaccurate statement, we will provide you with seven (7) days notice (for example, by posting the change on the Facebook Site Governance Page) and an opportunity to comment on changes to this Statement. You can also visit our Facebook Site Governance Page and "like" the Page to get updates about changes to this Statement.
2. If we make changes to policies referenced in or incorporated by this Statement, we may provide notice on the Site Governance Page.

3. Your continued use of Facebook following changes to our terms constitutes your acceptance of our amended terms.

15. **Termination**

If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account. You may also delete your account or disable your application at any time. In all such cases, this Statement shall terminate, but the following provisions will still apply: 2.2, 2.4, 3-5, 8.2, 9.1-9.3, 9.9, 9.10, 9.13, 9.15, 9.18, 10.3, 11.2, 11.5, 11.6, 11.9, 11.12, 11.13, and 15-19.

16. **Disputes**

1. You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in a state or federal court located in Santa Clara County. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims.
2. If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim. Although we provide rules for user conduct, we do not control or direct users' actions on Facebook and are not responsible for the content or information users transmit or share on Facebook. We are not responsible for any offensive, inappropriate, obscene, unlawful or otherwise objectionable content or information you may encounter on Facebook. We are not responsible for the conduct, whether online or offline, or any user of Facebook.
3. WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK AS IS WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE DO NOT GUARANTEE THAT FACEBOOK WILL ALWAYS BE SAFE, SECURE OR ERROR-FREE OR THAT FACEBOOK WILL ALWAYS FUNCTION WITHOUT DISRUPTIONS, DELAYS OR IMPERFECTIONS. FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES. IF YOU ARE A CALIFORNIA RESIDENT, YOU WAIVE CALIFORNIA CIVIL CODE §1542, WHICH SAYS: A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM MUST HAVE MATERIALLY AFFECTED HIS SETTLEMENT WITH THE DEBTOR. WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS ($100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS. APPLICABLE LAW MAY NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN SUCH CASES, FACEBOOK'S LIABILITY WILL BE LIMITED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW.

17. **Special Provisions Applicable to Users Outside the United States**

We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users and non-users who interact with Facebook outside the United States:

1. You consent to having your personal data transferred to and processed in the United States.
2. If you are located in a country embargoed by the United States, or are on the U.S. Treasury Department's list of Specially Designated Nationals you will not engage in commercial activities on Facebook (such as advertising or payments) or operate a Platform application or website.
3. Certain specific terms that apply only for German users are available here.

18. **Definitions**

1. By "Facebook" we mean the features and services we make available, including through (a) our website at www.facebook.com and any other Facebook branded or co-branded websites (including sub-domains, international versions, widgets, and mobile versions); (b) our Platform; (c) social plugins such as the Like button, the Share button and other similar offerings and (d) other media, software (such as a toolbar), devices, or networks now existing or later developed.
2. By "Platform" we mean a set of APIs and services (such as content) that enable others, including application developers and website operators, to retrieve data from Facebook or provide data to us.
3. By "information" we mean facts and other information about you, including actions taken by users and non-users who interact with Facebook.
4. By "content" we mean anything you or other users post on Facebook that would not be included in the definition of information.
5. By "data" or "user data" or "user's data" we mean any data, including a user's content or information that you or third parties can retrieve from Facebook or provide to Facebook through Platform.
6. By "post" we mean post on Facebook or otherwise make available by using Facebook.
7. By "use" we mean use, copy, publicly perform or display, distribute, modify, translate, and create derivative works of.
8. By "active registered user" we mean a user who has logged into Facebook at least once in the previous 30 days.
9. By "application" we mean any application or website that uses or accesses Platform, as well as anything else that receives or has received data from us. If you no longer access Platform but have not deleted all data from us, the term application will apply until you delete the data.

19. **Other**

1. If you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and Facebook Ireland Limited. References to “us,” “we,” and “our” mean either Facebook, Inc. or Facebook Ireland Limited, as appropriate.
2. This Statement makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements.
3. If any portion of this Statement is found to be unenforceable, the remaining portion will remain in full force and effect.
4. If we fail to enforce any of this Statement, it will not be considered a waiver.
5. Any amendment to or waiver of this Statement must be made in writing and signed by us.
6. You will not transfer any of your rights or obligations under this Statement to anyone else without our consent.
7. All of our rights and obligations under this Statement are freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise.
8. Nothing in this Statement shall prevent us from complying with the law.
9. This Statement does not confer any third party beneficiary rights.

10. We reserve all rights not expressly granted to you.
11. You will comply with all applicable laws when using or accessing Facebook.

You may also want to review the following documents, which provide additional information about your use of Facebook:

- Data Use Policy: The Data Use Policy contains information to help you understand how we collect and use information.
- Payment Terms: These additional terms apply to all payments made on or through Facebook.
- Platform Page: This page helps you better understand what happens when you add a third-party application or use Facebook Connect, including how they may access and use your data.
- Facebook Platform Policies: These guidelines outline the policies that apply to applications, including Connect sites.
- Advertising Guidelines: These guidelines outline the policies that apply to advertisements placed on Facebook.
- Promotions Guidelines: These guidelines outline the policies that apply if you offer contests, sweepstakes, and other types of promotions on Facebook.
- Brand Permissions Center: These guidelines outline the policies that apply to use of Facebook trademarks, logos and screenshots.
- How to Report Claims of Intellectual Property Infringement
- Pages Terms: These guidelines apply to your use of Facebook Pages.
- Community Standards: These guidelines outline our expectations regarding the content you post to Facebook and your activity on Facebook.

To access the Statement of Rights and Responsibilities in several different languages, change the language setting for your Facebook session by clicking on the language link in the left corner of most pages. If the Statement is not available in the language you select, we will default to the English version.

EXHIBIT B

Data Use Policy

Date of Last Revision: November 15, 2013

Information we receive and how it is used

- Information we receive about you
- Public information
- Usernames and User IDs
- How we use the information we receive
- Deleting and deactivating your account

Sharing and finding you on Facebook

- Control each time you post
- Control over your timeline
- Finding you on Facebook
- Access on phones and other devices
- Activity log
- What your friends and others share about you
- Groups
- Pages

Other websites and applications

- About Facebook Platform
- Controlling what information you share with applications
- Controlling what is shared when the people you share with use applications
- Logging in to another site using Facebook
- About social plugins
- About instant personalization
- Public search engines

Advertising and Facebook content

- Advertising
- Facebook content

Cookies, pixels and other similar technologies

Some other things you need to know

I. Information we receive and how it is used

Information we receive about you

We receive a number of different types of information about you, including:

Your information

Your information is the information that's required when you sign up for the site, as well as the information you choose to share.

- **Registration information**: When you sign up for Facebook, you are required to provide information such as your name, email address, birthday, and gender. In some cases, you may be able to register using other information, like your telephone number.

- **Information you choose to share**: Your information also includes the information you choose to share on Facebook, such as when you post a status update, upload a photo, or comment on a friend's story.

It also includes the information you choose to share when you communicate with us, such as when you contact us using an email address, or when you take an action, such as when you add a friend, like a Page or a website, add a place to your story, use our contact importers, or indicate you are in a relationship.

Your name, profile pictures, cover photos, gender, networks, username and User ID are treated just like information you choose to make public.
Your birthday allows us to do things like show you age-appropriate content and advertisements.

Information others share about you

We receive information about you from your friends and others, such as when they upload your contact information, post a photo of you, tag you in a photo or status update, or at a location, or add you to a group.

When people use Facebook, they may store and share information about you and others that they have, such as when they upload and manage their invites and contacts.

Other information we receive about you

We also receive other types of information about you:

- We receive data about you whenever you use or are running Facebook, such as when you look at another person's timeline, send or receive a message, search for a friend or a Page, click on, view or otherwise interact with things, use a Facebook mobile app, or make purchases through Facebook.
- When you post things like photos or videos on Facebook, we may receive additional related data (or metadata), such as the time, date, and place you took the photo or video.
- We receive data from or about the computer, mobile phone, or other devices you use to install Facebook apps or to access Facebook, including when multiple users log in from the same device. This may include network and communication information, such as your IP address or mobile phone number, and other information about things like your internet service, operating system, location, the type (including identifiers) of the device or browser you use, or the pages you visit. For example, we may get your GPS or other location information so we can tell you if any of your friends are nearby, or we could request device information to improve how our apps work on your device.
- We receive data whenever you visit a game, application, or website that uses Facebook Platform or visit a site with a Facebook feature (such as a social plugin), sometimes through cookies. This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your User ID.
- Sometimes we get data from our affiliates or our advertising partners, customers and other third parties that helps us (or them) deliver ads, understand online activity, and generally make Facebook better. For example, an

advertiser may tell us information about you (like how you responded to an ad on Facebook or on another site) in order to measure the effectiveness of - and improve the quality of - ads.

As described in "How we use the information we receive" we also put together data from the information we already have about you, your friends, and others, so we can offer and suggest a variety of services and features. For example, we may make friend suggestions, pick stories for your News Feed, or suggest people to tag in photos. We may put together your current city with GPS and other location information we have about you to, for example, tell you and your friends about people or events nearby, or offer deals to you in which you might be interested. We may also put together data about you to serve you ads or other content that might be more relevant to you.

When we get your GPS location, we put it together with other location information we have about you (like your current city). But we only keep it until it is no longer useful to provide you services, like keeping your last GPS coordinates to send you relevant notifications.
We only provide data to our advertising partners or customers after we have removed your name and any other personally identifying information from it, or have combined it with other people's data in a way that it no longer personally identifies you.

Public information

When we use the phrase "public information" (which we sometimes refer to as "Everyone information"), we mean the information you choose to make public, as well as information that is always publicly available.

Information you choose to make public
Choosing to make your information public is exactly what it sounds like: **anyone**, including people off Facebook, will be able to see it. Learn more.

Choosing to make your information public also means that this information:

- can be associated with you (i.e., your name, profile pictures, cover photos, timeline, User ID, username, etc.) even off Facebook;
- can show up when someone does a search on Facebook or on a public search engine;
- will be accessible to the Facebook-integrated games, applications, and websites you and your friends use; and
- will be accessible to anyone who uses our APIs such as our Graph API.

Sometimes you will not be able to select an audience when you post something (like when you write on a Page's wall or comment on a news article that uses our comments plugin). This is because some types of stories are always public stories. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available.
When others share information about you, they can also choose to make it public.

Information that is always publicly available
The types of information listed below are always publicly available, and they are treated just like information you decided to make public:

- **Name**: This helps your friends and family find you. If you are uncomfortable sharing your real name, you can always delete your account.

- **Profile Pictures and Cover Photos**: These help your friends and family recognize you. If you are uncomfortable making any of these photos public, you can always delete them. Unless you delete them, when you add a new profile picture or cover photo, the previous photo will remain public in your profile picture or cover photo album.

- **Networks**: This helps you see who you will be sharing information with before you choose "Friends and Networks" as a custom audience. If you are uncomfortable making your network public, you can leave the network.

- **Gender**: This allows us to refer to you properly.

- **Username and User ID**: These allow you to give out a custom link to your timeline or Page, receive email at your Facebook email address, and help make Facebook Platform possible.

Usernames and User IDs

Usernames and User IDs are the same thing – a way to identify you on Facebook. A User ID is a string of numbers and a username generally is some variation of your name. With your username, you get a custom link (a Facebook URL, such as www.facebook.com/username) to your timeline that you can give out to people or post on external websites.

If someone has your Username or User ID, they can use it to access information about you through the facebook.com website. For example, if someone has your Username, they can type facebook.com/Username into their browser and see your public information as well as anything else you've let them see. Similarly, someone with your Username or User ID can access information about you through our APIs, such as our Graph API. Specifically, they can access your public information, along with your age range, language and country.

If you do not want your information to be accessible to Platform applications, you can turn off all Platform applications from your Privacy Settings. If you turn off Platform you will no longer be able to use any games or other applications until you turn Platform back on. For more information about the information that apps receive when you visit them, see Other websites and applications.

If you want to see information available about you through our Graph API, just type **https://graph.facebook.com/[User ID or Username]?metadata=1** into your browser.
Your Facebook email address includes your public username like so: username@facebook.com. People can use your Facebook email address to send you messages and anyone in a message conversation can reply to it.

How we use the information we receive

We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use. For example, in addition to helping people see and find things that you do and share, we may use the information we receive about you:

- as part of our efforts to keep Facebook products, services and integrations safe and secure;
- to protect Facebook's or others' rights or property;
- to provide you with location features and services, like telling you and your friends when something is going on nearby;
- to measure or understand the effectiveness of ads you and others see, including to deliver relevant ads to you;
- to make suggestions to you and other users on Facebook, such as: suggesting that your friend use our contact importer because you found friends using it, suggesting that another user add you as a friend because the user imported the same email address as you did, or suggesting that your friend tag you in a picture they have uploaded with you in it; and
- for internal operations, including troubleshooting, data analysis, testing, research and service improvement.

Granting us permission to use your information not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways.

While you are allowing us to use the information we receive about you, you always own all of your information. Your trust is important to us, which is why we don't share information we receive about you with others unless we have:

- received your permission;
- given you notice, such as by telling you about it in this policy; or
- removed your name and any other personally identifying information from it.

Of course, for information others share about you, they control how it is shared.

We store data for as long as it is necessary to provide products and services to you and others, including those described above. Typically, information associated with your account will be kept until your account is deleted. For certain categories of data, we may also tell you about specific data retention practices.

We may enable access to public information that has been shared through our services.

We may allow service providers to access information so they can help us provide services.

We are able to suggest that your friend tag you in a picture by scanning and comparing your friend's pictures to information we've put together from your profile pictures and the other photos in which you've been tagged. If this feature is enabled for you, you can control whether we suggest that another user tag you in a photo using the "Timeline and Tagging" settings. Learn more at: https://www.facebook.com/help/tag-suggestions

Deleting and deactivating your account

If you want to stop using your account, you can either **deactivate** or **delete** it.

Deactivate

Deactivating your account puts your account on hold. Other users will no longer see your timeline, but we do not delete any of your information. Deactivating an account is the same as you telling us not to delete any information because you might want to reactivate your account at some point in the future. You can deactivate your account at: https://www.facebook.com/settings?tab=security
Your friends will still see you listed in their list of friends while your account is deactivated.

Deletion

When you delete your account, it is permanently deleted from Facebook. It typically takes about one month to delete an account, but some information may remain in backup copies and logs for up to 90 days. You should only delete your account if you are sure you never want to reactivate it. You can delete your account at: https://www.facebook.com/help/contact.php?show_form=delete_account
Learn more at: https://www.facebook.com/help/?faq=356107851084108

Certain information is needed to provide you with services, so we only delete this information after you delete your account. Some of the things you do on Facebook aren't stored in your account, like posting to a group or sending someone a message (where your friend may still have a message you sent, even after you delete your account). That information remains after you delete your account.

II. Sharing and finding you on Facebook

Control each time you post

Whenever you post content (like a status update, photo or check-in), you can select a specific audience, or even customize your audience. To do this, simply click on the sharing icon and choose who can see it.

Choose this icon if you want to make something **Public**. Choosing to make something public is exactly what it sounds like. It means that anyone, including people off Facebook, will be able to see or access it.
Choose this icon if you want to share with your Facebook **Friends**.
Choose this icon if you want to **Customize** your audience. You can also use this to hide your story from specific people.

If you tag someone, that person and their friends can see your story no matter what audience you selected. The same is true when you approve a tag someone else adds to your story.

Always think before you post. Just like anything else you post on the web or send in an email, information you share on

Facebook can be copied or re-shared by anyone who can see it.

Although you choose with whom you share, there may be ways for others to determine information about you. For example, if you hide your birthday so no one can see it on your timeline, but friends post “happy birthday!” on your timeline, people may determine your birthday.
When you comment on or "like" someone else's story, or write on their timeline, that person gets to select the audience. For example, if a friend posts a Public story and you comment on it, your comment will be Public. Often, you can see the audience someone selected for their story before you post a comment; however, the person who posted the story may later change their audience. So, if you comment on a story, and the story’s audience changes, the new audience can see your comment.
You can control who can see the Facebook Pages you've "liked" by visiting your timeline, clicking on the Likes box on your timeline, and then clicking "Edit."
Sometimes you will not see a sharing icon when you post something (like when you write on a Page's wall or comment on a news article that uses our comments plugin). This is because some types of stories are always public stories. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available.

Control over your timeline

Whenever you add things to your timeline you can select a specific audience, or even customize your audience. To do this, simply click on the sharing icon and choose who can see it.

Choose this icon if you want to make something **Public**. Choosing to make something public is exactly what it sounds like. It means that anyone, including people off Facebook, will be able to see or access it.
Choose this icon if you want to share with your Facebook **Friends**.
Choose this icon if you want to **Customize** your audience. You can also use this to hide the item on your timeline from specific people.

When you select an audience for your friend list, you are only controlling who can see the entire list of your friends on your timeline. We call this a timeline visibility control. This is because your friend list is always available to the games, applications and websites you use, and your friendships may be visible elsewhere (such as on your friends' timelines or in searches). For example, if you select "Only Me" as the audience for your friend list, but your friend sets her friend list to "Public," anyone will be able to see your connection on your friend's timeline.

Similarly, if you choose to hide your gender, it only hides it on your timeline. This is because we, just like the applications you and your friends use, need to use your gender to refer to you properly on the site.

When someone tags you in a story (such as a photo, status update or check-in), you can choose whether you want that story to appear on your timeline. You can either approve each story individually or approve all stories by your friends. If you approve a story and later change your mind, you can remove it from your timeline.

When you hide things on your timeline, like posts or connections, it means those things will not appear on your timeline. But, remember, anyone in the audience of those posts or who can see a connection may still see it elsewhere, like on someone else's timeline or in search results. You can also delete your posts or change the audience of content you post, which means you can remove people from or add people to the audience of the content.
People on Facebook may be able to see mutual friends, even if they cannot see your entire list of friends.
Some things (like your name, profile pictures and cover photos) do not have sharing icons because they are always publicly available. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available.

Finding you on Facebook

To make it easier for your friends to find you, we allow anyone with your contact information (such as email address or telephone number) to find you through the Facebook search bar at the top of most pages, as well as other tools we provide, such as contact importers - even if you have not shared your contact information with them on Facebook.

You can choose who can look up your timeline using the email address or telephone number you added to your timeline through your Privacy Settings. But remember that people can still find you or a link to your timeline on Facebook through other people and the things they share about you or through other posts, like if you are tagged in a friend's photo or post something to a public page.

Your settings do not control whether people can find you or a link to your timeline when they search for content they have permission to see, like a photo or other story in which you've been tagged.

Access on phones and other devices

Once you share information with your friends and others, they may be able to sync it with or access it via their mobile phones and other devices. For example, if you share a photo on Facebook, someone viewing that photo could save it using Facebook tools or by other methods offered by their device or browser. Similarly, if you share your contact information with someone or invite someone to an event, they may be able to use Facebook or third party applications or devices to sync that information. Or, if one of your friends has a Facebook application on one of their devices, your information (such as the things you post or photos you share) may be stored on or accessed by their device.

You should only share information with people you trust because they will be able to save it or re-share it with others, including when they sync the information to a device.

Activity log

Your activity log is a place where you can go to view most of your information on Facebook, including things you've hidden from your timeline. You can use this log to manage your content. For example, you can do things like delete stories, change the audience of your stories or stop an application from publishing to your timeline on your behalf.

When you hide something from your timeline, you are not deleting it. This means that the story may be visible elsewhere, like in your friends' News Feed. If you want to delete a story you posted, choose the delete option.

What your friends and others share about you

Links and Tags

Anyone can add a link to a story. Links are references to something on the Internet; anything from a website to a Page or timeline on Facebook. For example, if you are writing a story, you might include a link to a blog you are referencing or a link to the blogger's Facebook timeline. If someone clicks on a link to another person's timeline, they'll only see the things that they are allowed to see.

A tag is a special type of link to someone's timeline that suggests that the tagged person add your story to their timeline. In cases where the tagged person isn't included in the audience of the story, it will add them so they can see it. Anyone can tag you in anything. Once you are tagged, you and your friends will be able to see it (such as in News Feed or in search).

You can choose whether a story you've been tagged in appears on your timeline. You can either approve each story individually or approve all stories by your friends. If you approve a story and later change your mind, you can always remove it from your timeline.

If you do not want someone to tag you, we encourage you to reach out to them and give them that feedback. If that does not work, you can block them. This will prevent them from tagging you going forward.

Social reporting is a way for people to quickly and easily ask for help from someone they trust. Learn more at: https://www.facebook.com/note.php?note_id=196124227075034&__adt=3&__att=iframe

If you are linked to in a private space (such as a message or a group) only the people who can see the private space can see the link. Similarly, if you are linked to a comment, only the people who can see the comment can see the link.

Other information

As described in the "what your friends and others share about you" section of this policy, your friends and others may share information about you. They may share photos or other information about you and tag you in their posts. If you do not like a particular post, tell them or report the post.

Groups

Once you are in a Group, anyone in that Group can add you to a subgroup. When someone adds you to a Group, you will be listed as “invited” until you visit the Group. You can always leave a Group, which will prevent others from adding you to it again.

Pages

Facebook Pages are public pages. Companies use Pages to share information about their products. Celebrities use Pages to talk about their latest projects. And communities use Pages to discuss topics of interest, everything from baseball to the opera.

Because Pages are public, information you share with a Page is public information. This means, for example, that if you post a comment on a Page, that comment may be used by the Page owner off Facebook, and anyone can see it.

When you "like" a Page, you create a connection to that Page. The connection is added to your timeline and your friends may see it in their News Feeds. You may be contacted by or receive updates from the Page, such as in your News Feed and your messages. You can remove the Pages you've "liked" through your timeline or on the Page.

Some Pages contain content that comes directly from the Page owner. Page owners can do this through online plugins, such as an iframe, and it works just like the games and other applications you use through Facebook. Because this content comes directly from the Page owner, that Page may be able to collect information about you, just like any website.

Page administrators may have access to insights data, which will tell them generally about the people that visit their Page (as opposed to information about specific people). They may also know when you’ve made a connection to their Page because you’ve liked their Page or posted a comment.

To control who can see the Facebook Pages you've liked, visit our Help Center.

III. Other websites and applications

About Facebook Platform

Facebook Platform (or simply Platform) refers to the way we help you share your information with the games, applications, and websites you and your friends use. Facebook Platform also lets you bring your friends with you, so you can connect with them off Facebook. In these two ways, Facebook Platform helps you make your experiences on the web more personalized and social.

Remember that these games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook, so you should always make sure to read their terms of service and privacy policies to understand how they treat your data.

Controlling what information you share with applications

When you connect with a game, application or website - such as by going to a game, logging in to a website using your Facebook account, or adding an app to your timeline - we give the game, application, or website (sometimes referred to as just "applications" or "apps") your basic info (we sometimes call this your "public profile"), which includes your User ID and your public information. We also give them your friends' User IDs (also called your friend list) as part of your basic info.

Your friend list helps the application make your experience more social because it lets you find your friends on that application. Your User ID helps the application personalize your experience because it can connect your account on that application with your Facebook account, and it can access your basic info, which includes your public information and friend list. This includes the information you choose to make public, as well as information that is always publicly available. If the application needs additional information, such as your stories, photos or likes, it will have to ask you for specific permission.

The "Apps" setting lets you control the applications you use. You can see the permissions you have given these applications, the last time an application accessed your information, and the audience on Facebook for timeline stories and activity the application posts on your behalf. You can also remove applications you no longer want, or turn off all Platform applications. When you turn all Platform applications off, your User ID is no longer given to applications, even when your friends use those applications. But you will no longer be able to use any games, applications or websites through Facebook.

When you first visit an app, Facebook lets the app know your language, your country, and whether you are in an age group, for instance, under 18, between 18-20, or 21 and over. Age range lets apps provide you with age-appropriate content. If you install the app, it can access, store and update the information you've shared. Apps you've installed can update their records of your basic info, age range, language and country. If you haven't used an app in a while, you should consider removing it. Once you remove an app, it won't be able to continue to update the additional information you've given them permission to access, but it may still hold the information you have already shared. You always can contact the app directly and request that they delete your data. Learn more at: https://www.facebook.com/help/how-apps-work

Sometimes a game console, mobile phone, or other device might ask for permission to share specific information with the games and applications you use on that device. If you say okay, those applications will not be able to access any other information about you without asking specific permission from you or your friends.

Sites and apps that use Instant Personalization receive your User ID and friend list when you visit them.

You always can remove apps you've installed by using your app settings at: https://www.facebook.com/settings/?tab=applications. But remember, apps may still be able to access your information when the people you share with use them. And, if you've removed an application and want it to delete the information you've already shared with it, you should contact the application. Visit the application's page on Facebook or its own website to learn more about the app. For example, Apps may have reasons (e.g. legal obligations) to retain some data that you share with them.

Controlling what is shared when the people you share with use applications

Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use.

Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social. For example, one of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of that application, your friend would want to give the application her friend list – which includes your User ID – so the application knows which of her friends is also using it. Your friend might also want to share the music you "like" on Facebook. If you have made that information public, then the application can access it just like anyone else. But if you've shared your likes with just your friends, the application could ask your friend for permission to share them.

You can control most of the information other people can share with applications they use from the "App" settings page. But these controls do not let you limit access to your public information and friend list.

If you want to completely block applications from getting your information when your friends and others use them, you will need to turn off all Platform applications. This means that you will no longer be able to use any third-party Facebook-integrated games, applications or websites.

If an application asks permission from someone else to access your information, the application will be allowed to use

that information only in connection with the person that gave the permission, and no one else.

For example, some apps use information such as your friends list, to personalize your experience or show you which of your friends use that particular app.

Logging in to another site using Facebook

Facebook Platform lets you log into other applications and websites using your Facebook account. When you log in using Facebook, we give the site your User ID (just like when you connect with any other application), but we do not share your email address or password with that website through this process without your permission.

If you already have an account on that website, the site may also be able to connect that account with your Facebook account. Sometimes it does this using what is called an "email hash", which is similar to searching for someone on Facebook using an email address. Only the email addresses in this case are hashed so no email addresses are actually shared between Facebook and the website.

How it works

The website sends over a hashed version of your email address, and we match it with a database of email addresses that we have also hashed. If there is a match, then we tell the website the User ID associated with the email address. This way, when you log into the website using Facebook, the website can link your Facebook account to your account on that website.

About social plugins

Social plugins are buttons, boxes, and stories (such as the Like button) that other websites can use to present Facebook content to you and create more social and personal experiences for you. While you view these buttons, boxes, and stories on other sites, the content comes directly from Facebook.

Sometimes plugins act just like applications. You can spot one of these plugins because it will ask you for permission to access your information or to publish information back to Facebook. For example, if you use a registration plugin on a website, the plugin will ask your permission to share your basic info with the website to make it easier for you to register for the website. Similarly, if you use an "Add To Timeline" plugin, the plugin will ask for your permission to publish stories about your activities on that website to Facebook.

If you make something public using a plugin, such as posting a public comment on a newspaper's website, then that website can access your comment (along with your User ID) just like everyone else.

If you post something using a social plugin and you do not see a sharing icon, you should assume that story is Public. For example, if you post a comment through a Facebook comment plugin on a site, your story is Public and everyone, including the website, can see your story.

Websites that use social plugins can sometimes tell that you have engaged with the social plugin. For example, they may know that you clicked on a Like button in a social plugin.

We receive data when you visit a site with a social plugin. We keep this data for a maximum of 90 days. After that, we remove your name and any other personally identifying information from the data, or combine it with other people's data in a way that it is no longer associated with you. Learn more at: https://www.facebook.com/help/social-plugins

About instant personalization

Instant personalization (sometimes also referred to as "Start now") is a way for Facebook to help partners (such as Bing and Rotten Tomatoes) on and off Facebook to create a more personalized and social experience for logged in users than a social plugin can offer. When you visit a site or app using instant personalization, it will know some information about you and your friends the moment you arrive. This is because sites and apps using instant personalization can access your User ID, your friend list, and your public information.

The first time you visit a site or app using instant personalization, you will see a notification letting you know that the

site or app has partnered with Facebook to provide a personalized experience.

The notification will give you the ability to disable or turn off instant personalization for that site or app. If you do that, that site or app is required to delete all of the information about you it received from Facebook as part of the instant personalization program. In addition, we will prevent that site from accessing your information in the future, even when your friends use that site.

If you decide that you do not want to experience instant personalization for all partner sites and apps, you can disable instant personalization from the "Apps" settings page.

If you turn off instant personalization, these partner third party sites and apps will not be able to access your public information, even when your friends visit those sites.

If you turn off an instant personalization site or app after you have been using it or visited it a few times (or after you have given it specific permission to access your data), it will not automatically delete information about you it received through Facebook. Like all other apps, the site is required by our policies to delete information about you if you ask it to do so.

How it works

To join the instant personalization program, a potential partner must enter into an agreement with us designed to protect your privacy. For example, this agreement requires that the partner delete information about you if you turn off instant personalization when you first visit the site or app. It also prevents the partner from accessing any information about you until you or your friends visit its site.

Instant personalization partners sometimes use an email hash process to see if any of their users are on Facebook and get those users' User IDs. This process is similar to searching for someone on Facebook using an email address, except in this case, the email addresses are hashed so no actual email addresses are exchanged. The partner is also contractually required not to use your User ID for any purpose (other than associating it with your account) until you or your friends visit the site.

When you visit a site or app using instant personalization, we provide the site or app with your User ID and your friend list (as well as your age range, locale, and gender). The site or app can then connect your account with your friends' accounts to make the site or app instantly social. The site can also access public information associated with any of the User IDs it receives, which it can use to make them instantly personalized. For example, if the site is a music site, it can access your music interests to suggest songs you may like, and access your friends' music interests to let you know what they are listening to. Of course it can only access your or your friends' music interests if they are public. If the site or app wants any additional information, it will have to get your specific permission.

Public search engines

Your public search setting controls whether people who enter your name on a public search engine may see your public timeline (including in sponsored results). You can find your public search setting on the "Privacy Settings and Tools" settings page.

This setting does not apply to search engines that access your information as an application using Facebook Platform. If you turn your public search setting off and then search for yourself on a public search engine, you may still see a preview of your timeline. This is because some search engines cache information for a period of time. You can learn more about how to request a search engine to remove you from cached information at: https://www.facebook.com/help/?faq=13323

IV. Advertising and Facebook content

Advertising

Facebook offers a range of products that allow advertisers to reach people on and off Facebook. In addition to the

information we provide in this section, you can also learn more about advertising products, how they work, our partnerships, and the controls you have, by visiting our "Advertising on Facebook" page.

When we deliver ads, we do not share your information (information that personally identifies you, such as your name or contact information) with advertisers unless you give us permission. We may provide advertisers with information when we have removed your name and other personally identifying information from it, or combined it with other information so that it no longer personally identifies you. For example, we may tell an advertiser how its ads perform or how many people viewed or clicked on their ads or install an app after seeing an ad.

So we can show you content that you may find interesting, we may use all of the information we receive about you to serve ads that are more relevant to you. For example, this includes:

- information you provide at registration or add to your account or timeline,
- things you share and do on Facebook, such as what you like, and your interactions with advertisements, partners, or apps,
- keywords from your stories, and
- things we infer from your use of Facebook.

For many ads we serve, advertisers may choose their audience by location, demographics, likes, keywords, and any other information we receive or infer about users. Here are some of the ways advertisers may target relevant ads:

- demographics and interests: for example, 18 to 35 year-old women who live in the United States and like basketball;
- topics or keywords: for example, "music" or people who like a particular song or artist;
- Page likes (including topics such as products, brands, religion, health status, or political views): for example, if you like a Page about gluten-free food, you may receive ads about relevant food products; or
- categories (including things like "moviegoer" or a "sci-fi fan"): for example, if a person "likes" the "Star Trek" Page and mentions "Star Wars" when they check into a movie theater, we may infer that this person is likely to be a sci-fi fan and advertisers of sci-fi movies could ask us to target that category.

In addition to delivering relevant ads, Facebook sometimes pairs ads with social context, meaning stories about social actions that you or your friends have taken. For example, an ad for a sushi restaurant's Facebook Page may be paired with a News Feed story that one of your friends likes that Page.

We also sometimes serve these same types of ads on other sites or may serve just the social context (such as with ads served by others), so that the ads are more relevant to you. Just like any other content you share on Facebook, only people who you're already sharing with on Facebook would see it when it is paired with an ad. We also allow advertisers to reach people on Facebook using the information they already have about you (such as email addresses or whether you have visited their websites previously). You can learn more about ads, social context, and our partnerships, including the relevant settings and controls available to you, by visiting the Advertising on Facebook page.

If an advertiser chooses to run ads, we serve the ads to people who meet criteria the advertiser selects. So, if someone views or otherwise interacts with the ad, the advertiser might assume that the person meets the criteria they selected (for example, that the person is an 18-to-35-year-old woman who lives in the U.S. and likes basketball). We require advertisers to comply with our Advertising Guidelines, including provisions relating to the use of sensitive data.

Advertisers and their partners sometimes use cookies or other similar technologies in order to serve and measure ads and to make their ads more effective. Learn more about cookies, pixels and similar technologies.

When you post a story on Facebook and an advertiser sponsors it, nothing changes about the audience of the post. Only the people who could originally see the post (the people you shared it with) are eligible to see it.

Facebook content

We like to tell you about some of the features and tools your friends and others use on Facebook, to help you have a

better experience. For example, if your friend uses our friend finder tool to find more friends on Facebook, we may tell you about it to encourage you to use it as well. This of course means your friend may similarly see suggestions based on the things you do. But we will try to only show it to friends that could benefit from your experience.

V. Cookies, pixels and other similar technologies

Cookies are small pieces of data that are stored on your computer, mobile phone or other device. Pixels are small blocks of code on webpages that do things like allow another server to measure viewing of a webpage and often are used in connection with cookies.

We use technologies like cookies, pixels, and local storage (like on your browser or device, which is similar to a cookie but holds more information) to provide and understand a range of products and services. Learn more at: https://www.facebook.com/help/cookies

We use these technologies to do things like:

- make Facebook easier or faster to use;
- enable features and store information about you (including on your device or in your browser cache) and your use of Facebook;
- deliver, understand and improve advertising;
- monitor and understand the use of our products and services; and
- protect you, others and Facebook.

For example, we may use these tools to know you are logged in to Facebook, to help you use social plugins and share buttons, or to know when you are interacting with our advertising or Platform partners.

We may ask advertisers or other partners to serve ads or services to computers, mobile phones or other devices, which may use a cookie, pixel or other similar technology placed by Facebook or the third party (although we would not share information that personally identifies you with an advertiser).

Most companies on the web use cookies (or other similar technological tools), including our advertising and Platform partners. For example, our Platform partners, advertisers or Page administrators may use cookies or similar technologies when you access their apps, ads, Pages or other content.

Cookies and things like local storage help make Facebook work, like allowing pages to load faster because certain content is stored on your browser or by helping us authenticate you to deliver personalized content.
To learn more about how advertisers generally use cookies and the choices advertisers provide, visit the Network Advertising Initiative at http://www.networkadvertising.org/managing/opt_out.asp, the Digital Advertising Alliance at http://www.aboutads.info/, the Internet Advertising Bureau (US) at http://www.iab.net or the Internet Advertising Bureau (EU) at http://youronlinechoices.eu/.
Refer to your browser or device's help material to learn what controls you can often use to remove or block cookies or other similar technologies or block or remove other data stored on your computer or device (such as by using the various settings in your browser). If you do this, it may affect your ability to use Facebook or other websites and apps.

VI. Some other things you need to know

Safe harbor

Facebook complies with the U.S.-EU and U.S.-Swiss Safe Harbor frameworks as set forth by the Department of Commerce regarding the collection, use, and retention of data from the European Union. To view our certification, visit the U.S. Department of Commerce's Safe Harbor website at: https://safeharbor.export.gov/list.aspx. As part of our participation in the Safe Harbor program, we agree to resolve disputes you have with us in connection with our policies and practices through TRUSTe. If you would like to contact TRUSTe, visit:https://feedback-form.truste.com/watchdog/request

Contact us with questions or disputes

If you have questions or complaints regarding our Data Use Policy or practices, please contact us by mail at 1601 Willow Road, Menlo Park, CA 94025 if you reside in the U.S. or Canada, or at Facebook Ireland Ltd., Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland if you live outside the U.S. or Canada. Anyone may also contact us through this help page: https://www.facebook.com/help/contact_us.php?id=173545232710000

Responding to legal requests and preventing harm

We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; or to prevent death or imminent bodily harm.

Information we receive about you, including financial transaction data related to purchases made with Facebook, may be accessed, processed and retained for an extended period of time when it is the subject of a legal request or obligation, governmental investigation, or investigations concerning possible violations of our terms or policies, or otherwise to prevent harm. We also may retain information from accounts disabled for violations of our terms for at least a year to prevent repeat abuse or other violations of our terms.

Access requests

You can access and correct most of your personal data stored by Facebook by logging into your account and viewing your timeline and activity log. You can also download a copy of your personal data by visiting your "Settings" (General Account Settings page), clicking on "Download a copy of your Facebook data" and then clicking on the link for your expanded archive. Learn more at: https://www.facebook.com/help/?faq=226281544049399

Notifications and Other Messages

We may send you notifications and other messages using the contact information we have for you, like your email address. You can control most of the notifications you receive, including ones from Pages you like and applications you use, using controls we provide, such as a control included in the email you receive or in your "Notifications" settings.

Friend Finder

We offer tools to help you upload your friends' contact information so that you and others can find friends on Facebook, and invite friends who do not use Facebook to join, and so we can offer you and others better experiences on Facebook through suggestions and other customized experiences. If you do not want us to store this information, visit this help page at: https://www.facebook.com/contact_importer/remove_uploads.php.

If you give us your password, we will delete it after you upload your friends' contact information.

Invitations

When you invite a friend to join Facebook, we send a message on your behalf using your name, and we may also include names and pictures of other people your friend might know on Facebook. We'll also send a few reminders to those you invite, but the invitation will also give your friend the opportunity to opt out of receiving other invitations to join Facebook.

Memorializing accounts

We may memorialize the account of a deceased person. When we memorialize an account, we keep the timeline on Facebook, but limit access and some features. You can report a deceased person's timeline at: https://www.facebook.com/help/contact.php?show_form=deceased

We also may close an account if we receive a formal request that satisfies certain criteria.

Affiliates

We may share information we receive with businesses that are legally part of the same group of companies that Facebook is part of, or that become part of that group (often these companies are called affiliates). Likewise, our

affiliates may share information with us as well. This sharing is done in compliance with applicable laws including where such applicable laws require consent. We and our affiliates may use shared information to help provide, understand, and improve our services and their own services.

Service Providers

We give your information to the people and companies that help us provide, understand and improve the services we offer. For example, we may use outside vendors to help host our website, serve photos and videos, process payments, analyze data, conduct and publish research, measure the effectiveness of ads, or provide search results. In some cases we provide the service jointly with another company, such as the Facebook Marketplace. In all of these cases our partners must agree to only use your information consistent with the agreement we enter into with them, as well as this Data Use Policy.

Security and bugs

We do our best to keep your information secure, but we need your help. For more detailed information about staying safe on Facebook, visit the Facebook Security Page. We try to keep Facebook up, bug-free and safe, but can't make guarantees about any part of our services or products.

Change of Control

If the ownership of our business changes, we may transfer your information to the new owner so they can continue to operate the service. But they will still have to honor the commitments we have made in this Data Use Policy.

Notice of Changes

If we make changes to this Data Use Policy we will notify you (for example, by publication here and on the Facebook Site Governance Page). If the changes are material, we will provide you additional, prominent notice as appropriate under the circumstances. You can make sure that you receive notice directly by liking the Facebook Site Governance Page.

Opportunity to comment

Unless we make a change for legal or administrative reasons, or to correct an inaccurate statement, we will give you seven (7) days to provide us with comments on the change. After the comment period, if we adopt any changes, we will provide notice (for example, on the Facebook Site Governance Page or in this policy) of the effective date.

Information for users outside of the United States and Canada

Company Information: The website under www.facebook.com and the services on these pages are being offered to users outside of the U.S. and Canada by Facebook Ireland Ltd., Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland. The company Facebook Ireland Ltd. has been established and registered in Ireland as a private limited company, Company Number: 462932, and is the data controller responsible for your personal information.
Directors: Sonia Flynn (Irish), Shane Crehan (Irish).

Your California privacy rights

California law permits residents of California to request certain details about what personal information a company shares with third parties for the third parties' direct marketing purposes. Facebook does not share your information with third parties for the third parties' own and independent direct marketing purposes unless we receive your permission. Learn more about the information we receive and how it is used and other websites and applications. If you have questions about our sharing practices or your rights under California law, please write us at 1601 Willow Road, Menlo Park,

Data Use Policy

Date of Last Revision: December 11, 2012

Information we receive and how it is used

- Information we receive about you
- Public information
- Usernames and User IDs
- How we use the information we receive
- Deleting and deactivating your account

Sharing and finding you on Facebook

- Control each time you post
- Control over your timeline
- Finding you on Facebook
- Access on phones and other devices
- Activity log
- What your friends and others share about you
- Groups
- Pages

Other websites and applications

- About Facebook Platform
- Controlling what information you share with applications
- Controlling what is shared when the people you share with use applications
- Logging in to another site using Facebook
- About social plugins
- About instant personalization
- Public search engines

How advertising and Sponsored Stories work

- Personalized ads
- Ads + social context
- Sponsored stories

- Facebook content

Cookies, pixels and other similar technologies
Some other things you need to know

I. Information we receive and how it is used

Information we receive about you

We receive a number of different types of information about you, including:

Your information
Your information is the information that's required when you sign up for the site, as well as the information you choose to share.

- **Registration information**: When you sign up for Facebook, you are required to provide information such as your name, email address, birthday, and gender. In some cases, you may be able to register using other information, like your telephone number.

- **Information you choose to share**: Your information also includes the information you choose to share on Facebook, such as when you post a status update, upload a photo, or comment on a friend's story.

It also includes the information you choose to share when you take an action, such as when you add a friend, like a Page or a website, add a place to your story, use our contact importers, or indicate you are in a relationship.

Your name, profile pictures, cover photos, gender, networks, username and User ID are treated just like information you choose to make public.
Your birthday allows us to do things like show you age-appropriate content and advertisements.

Information others share about you
We receive information about you from your friends and others, such as when they upload your contact information, post a photo of you, tag you in a photo or status update, or at a location, or add you to a group.

When people use Facebook, they may store and share information about you and others that they have, such as when they upload and manage their invites and contacts.

Other information we receive about you
We also receive other types of information about you:

- We receive data about you whenever you interact with Facebook, such as when you look at another person's timeline, send or receive a message, search for a friend or a Page, click on, view or otherwise interact with things, use a Facebook mobile app, or purchase Facebook Credits or make other purchases through Facebook.
- When you post things like photos or videos on Facebook, we may receive additional related data (or metadata), such as the time, date, and place you took the photo or video.
- We receive data from the computer, mobile phone or other device you use to access Facebook, including when multiple users log in from the same device. This may include your IP address and other information about things like your internet service, location, the type (including identifiers) of browser you use, or the pages you visit. For example, we may get your GPS or other location information so we can tell you if any of your friends are nearby.
- We receive data whenever you visit a game, application, or website that uses Facebook Platform or visit a site with a Facebook feature (such as a social plugin), sometimes through cookies. This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your User ID.
- Sometimes we get data from our affiliates or our advertising partners, customers and other third parties that helps us (or them) deliver ads, understand online activity, and generally make Facebook better. For example, an

advertiser may tell us information about you (like how you responded to an ad on Facebook or on another site) in order to measure the effectiveness of - and improve the quality of - ads.

We also put together data from the information we already have about you and your friends. For example, we may put together data about you to determine which friends we should show you in your News Feed or suggest you tag in the photos you post. We may put together your current city with GPS and other location information we have about you to, for example, tell you and your friends about people or events nearby, or offer deals to you that you might be interested in. We may also put together data about you to serve you ads that might be more relevant to you.

When we get your GPS location, we put it together with other location information we have about you (like your current city). But we only keep it until it is no longer useful to provide you services, like keeping your last GPS coordinates to send you relevant notifications.
We only provide data to our advertising partners or customers after we have removed your name or any other personally identifying information from it, or have combined it with other people's data in a way that it is no longer associated with you.

Public information

When we use the phrase "public information" (which we sometimes refer to as "Everyone information"), we mean the information you choose to make public, as well as information that is always publicly available.

Information you choose to make public

Choosing to make your information public is exactly what it sounds like: **anyone**, including people off of Facebook, will be able to see it.

Choosing to make your information public also means that this information:

- can be associated with you (i.e., your name, profile pictures, cover photos, timeline, User ID, username, etc.) even off Facebook;
- can show up when someone does a search on Facebook or on a public search engine;
- will be accessible to the Facebook-integrated games, applications, and websites you and your friends use; and
- will be accessible to anyone who uses our APIs such as our Graph API.

Sometimes you will not be able to select an audience when you post something (like when you write on a Page's wall or comment on a news article that uses our comments plugin). This is because some types of stories are always public stories. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available.
When others share information about you, they can also choose to make it public.

Information that is always publicly available

The types of information listed below are always publicly available, and are treated just like information you decided to make public.

- **Name**: This helps your friends and family find you. If you are uncomfortable sharing your real name, you can always delete your account.

- **Profile Pictures and Cover Photos**: These help your friends and family recognize you. If you are uncomfortable making any of these photos public, you can always delete it. Unless you delete them, when you add a new profile picture or cover photo, the previous photo will remain public in your profile picture or cover photo album.

- **Networks**: This helps you see whom you will be sharing information with before you choose "Friends and Networks" as a custom audience. If you are uncomfortable making your network public, you can leave the network.

- **Gender**: This allows us to refer to you properly.

- **Username and User ID**: These allow you to give out a custom link to your timeline or Page, receive email at your Facebook email address, and help make Facebook Platform possible.

Usernames and User IDs

A Username (or Facebook URL) is a custom link to your timeline that you can give out to people or post on external websites. Usernames appear in the URL on your timeline. We also use your User ID to identify your Facebook account.

If someone has your Username or User ID, they can use it to access information about you through the facebook.com website. For example, if someone has your Username, they can type facebook.com/Username into their browser and see your public information as well as anything else you've let them see. Similarly, someone with your Username or User ID can access information about you through our APIs, such as our Graph API. Specifically, they can access your public information, along with your age range, language and country.

If you do not want your information to be accessible to Platform applications, you can turn off all Platform applications from your Privacy Settings. If you turn off Platform you will no longer be able to use any games or other applications until you turn Platform back on. For more information about the information that apps receive when you visit them, see Other websites and applications.

If you want to see information available about you through our Graph API, just type **https://graph.facebook.com/[User ID or Username]?metadata=1** into your browser.
Your Facebook email address includes your public username like so: username@facebook.com. Anyone in a message conversation can reply to it.

How we use the information we receive

We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use. For example, in addition to helping people see and find things that you do and share, we may use the information we receive about you:

- as part of our efforts to keep Facebook products, services and integrations safe and secure;
- to protect Facebook's or others' rights or property;
- to provide you with location features and services, like telling you and your friends when something is going on nearby;
- to measure or understand the effectiveness of ads you and others see, including to deliver relevant ads to you;
- to make suggestions to you and other users on Facebook, such as: suggesting that your friend use our contact importer because you found friends using it, suggesting that another user add you as a friend because the user imported the same email address as you did, or suggesting that your friend tag you in a picture they have uploaded with you in it; and
- for internal operations, including troubleshooting, data analysis, testing, research and service improvement.

Granting us this permission not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways.

While you are allowing us to use the information we receive about you, you always own all of your information. Your trust is important to us, which is why we don't share information we receive about you with others unless we have:

- received your permission;
- given you notice, such as by telling you about it in this policy; or
- removed your name or any other personally identifying information from it.

Of course, for information others share about you, they control how it is shared.

We store data for as long as it is necessary to provide products and services to you and others, including those described above. Typically, information associated with your account will be kept until your account is deleted. For certain categories of data, we may also tell you about specific data retention practices.

We are able to suggest that your friend tag you in a picture by scanning and comparing your friend's pictures to information we've put together from the other photos you've been tagged in. This allows us to make these suggestions. You can control whether we suggest that another user tag you in a photo using the “How Tags work” settings. Learn more at: https://www.facebook.com/help/tag-suggestions

Deleting and deactivating your account

If you want to stop using your account, you can either **deactivate** or **delete** it.

Deactivate

Deactivating your account puts your account on hold. Other users will no longer see your timeline, but we do not delete any of your information. Deactivating an account is the same as you telling us not to delete any information because you might want to reactivate your account at some point in the future. You can deactivate your account at: https://www.facebook.com/settings?tab=security
Your friends will still see you listed in their list of friends while your account is deactivated.

Deletion

When you delete an account, it is permanently deleted from Facebook. It typically takes about one month to delete an account, but some information may remain in backup copies and logs for up to 90 days. You should only delete your account if you are sure you never want to reactivate it. You can delete your account at: https://www.facebook.com/help/contact.php?show_form=delete_account
Learn more at: https://www.facebook.com/help/?faq=356107851084108

Certain information is needed to provide you with services, so we only delete this information after you delete your account. Some of the things you do on Facebook aren’t stored in your account, like posting to a group or sending someone a message (where your friend may still have a message you sent, even after you delete your account). That information remains after you delete your account.

II. Sharing and finding you on Facebook

Control each time you post

Whenever you post content (like a status update, photo or check-in), you can select a specific audience, or even customize your audience. To do this, simply click on the sharing icon and choose who can see it.

Choose this icon if you want to make something **Public**. Choosing to make something public is exactly what it sounds like. It means that anyone, including people off of Facebook, will be able to see or access it.
Choose this icon if you want to share with your Facebook **Friends**.
Choose this icon if you want to **Customize** your audience. You can also use this to hide your story from specific people.

If you tag someone, that person and their friends can see your story no matter what audience you selected. The same is true when you approve a tag someone else adds to your story.

Always think before you post. Just like anything else you post on the web or send in an email, information you share on Facebook can be copied or re-shared by anyone who can see it.

Although you choose with whom you share, there may be ways for others to determine information about you. For example, if you hide your birthday so no one can see it on your timeline, but friends post “happy birthday!” on your timeline, people may determine your birthday.
When you comment on or "like" someone else's story, or write on their timeline, that person gets to select the audience.

For example, if a friend posts a Public story and you comment on it, your comment will be Public. Often, you can see the audience someone selected for their story before you post a comment; however, the person who posted the story may later change their audience.
You can control who can see the Facebook Pages you've "liked" by visiting your timeline, clicking on the Likes box on your timeline, and then clicking "Edit."
Sometimes you will not see a sharing icon when you post something (like when you write on a Page's wall or comment on a news article that uses our comments plugin). This is because some types of stories are always public stories. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available.

Control over your timeline

Whenever you add things to your timeline you can select a specific audience, or even customize your audience. To do this, simply click on the sharing icon and choose who can see it.

Choose this icon if you want to make something **Public**. Choosing to make something public is exactly what it sounds like. It means that anyone, including people off of Facebook, will be able to see or access it.
Choose this icon if you want to share with your Facebook **Friends**.
Choose this icon if you want to **Customize** your audience. You can also use this to hide the item on your timeline from specific people.

When you select an audience for your friend list, you are only controlling who can see the entire list of your friends on your timeline. We call this a timeline visibility control. This is because your friend list is always available to the games, applications and websites you use, and your friendships may be visible elsewhere (such as on your friends' timelines or in searches). For example, if you select "Only Me" as the audience for your friend list, but your friend sets her friend list to "Public," anyone will be able to see your connection on your friend's timeline.

Similarly, if you choose to hide your gender, it only hides it on your timeline. This is because we, just like the applications you and your friends use, need to use your gender to refer to you properly on the site.

When someone tags you in a story (such as a photo, status update or check-in), you can choose whether you want that story to appear on your timeline. You can either approve each story individually or approve all stories by your friends. If you approve a story and later change your mind, you can remove it from your timeline.

When you hide things on your timeline, like posts or connections, it means those things will not appear on your timeline. But, remember, anyone in the audience of those posts or who can see a connection may still see it elsewhere, like on someone else's timeline or in search results. You can also delete or change the audience of content you post.
People on Facebook may be able to see mutual friends, even if they cannot see your entire list of friends.
Some things (like your name, profile pictures and cover photos) do not have sharing icons because they are always publicly available. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available.

Finding you on Facebook

To make it easier for your friends to find you, we allow anyone with your contact information (such as email address or telephone number) to find you through the Facebook search bar at the top of most pages, as well as other tools we provide, such as contact importers - even if you have not shared your contact information with them on Facebook.

You can choose who can look up your timeline using the email address or telephone number you added to your timeline through your privacy settings. But remember that people can still find you or a link to your timeline on Facebook through other people and the things they share about you or through other posts, like if you are tagged in a friend's photo or post something to a public page.

Your settings do not control whether people can find you or a link to your timeline when they search for content they have permission to see, like a photo or other story you've been tagged in.

Access on phones and other devices

Once you share information with your friends and others, they may be able to sync it with or access it via their mobile phones and other devices. For example, if you share a photo on Facebook, someone viewing that photo could save it using Facebook tools or by other methods offered by their device or browser. Similarly, if you share your contact information with someone or invite someone to an event, they may be able to use Facebook or third party applications or devices to sync that information. Or, if one of your friends has a Facebook application on one of their devices, your information (such as the things you post or photos you share) may be stored on or accessed by their device.

You should only share information with people you trust because they will be able to save it or re-share it with others, including when they sync the information to a device.

Activity log

Your activity log is a place where you can go to view most of your information on Facebook, including things you've hidden from your timeline. You can use this log to manage your content. For example, you can do things like delete stories, change the audience of your stories or stop an application from publishing to your timeline on your behalf.

When you hide something from your timeline, you are not deleting it. This means that the story may be visible elsewhere, like in your friends' News Feed. If you want to delete a story you posted, choose the delete option.

What your friends and others share about you

Links and Tags

Anyone can add a link to a story. Links are references to something on the Internet; anything from a website to a Page or timeline on Facebook. For example, if you are writing a story, you might include a link to a blog you are referencing or a link to the blogger's Facebook timeline. If someone clicks on a link to another person's timeline, they'll only see the things that they are allowed to see.

A tag is a special type of link to someone's timeline that suggests that the tagged person add your story to their timeline. In cases where the tagged person isn't included in the audience of the story, it will add them so they can see it. Anyone can tag you in anything. Once you are tagged, you and your friends will be able to see it (such as in News Feed or in search).

You can choose whether a story you've been tagged in appears on your timeline. You can either approve each story individually or approve all stories by your friends. If you approve a story and later change your mind, you can always remove it from your timeline.

If you do not want someone to tag you, we encourage you to reach out to them and give them that feedback. If that does not work, you can block them. This will prevent them from tagging you going forward.

If you are linked to or tagged in a private space (such as a message or a group) only the people who can see the private space can see the link or tag. Similarly, if you are linked to or tagged in a comment, only the people who can see the comment can see the link or tag.

Other information

As described in the what your friends and others share about you section of this policy, your friends and others may share information about you. They may share photos or other information about you and tag you in their posts. If you do not like a particular post, tell them or report the post.

Groups

Once you are in a Group, anyone in that Group can add you to a subgroup. When someone adds you to a Group, you will be listed as "invited" until you visit the Group. You can always leave a Group, which will prevent others from adding you to it again.

Pages

Facebook Pages are public pages. Companies use Pages to share information about their products. Celebrities use Pages to talk about their latest projects. And communities use pages to discuss topics of interest, everything from baseball to the opera.

Because Pages are public, information you share with a Page is public information. This means, for example, that if you post a comment on a Page, that comment may be used by the Page owner off Facebook, and anyone can see it.

When you "like" a Page, you create a connection to that Page. The connection is added to your timeline and your friends may see it in their News Feeds. You may be contacted by or receive updates from the Page, such as in your News Feed and your messages. You can remove the Pages you've "liked" through your timeline or on the Page.

Some Pages contain content that comes directly from the Page owner. Page owners can do this through online plugins, such as an iframe, and it works just like the games and other applications you use through Facebook. Because this content comes directly from the Page owner, that Page may be able to collect information about you, just like any website.

Page administrators may have access to insights data, which will tell them generally about the people that visit their Page (as opposed to information about specific people). They may also know when you've made a connection to their Page because you've liked their Page or posted a comment.

III. Other websites and applications

About Facebook Platform

Facebook Platform (or simply Platform) refers to the way we help you share your information with the games, applications, and websites you and your friends use. Facebook Platform also lets you bring your friends with you, so you can connect with them off of Facebook. In these two ways, Facebook Platform helps you make your experiences on the web more personalized and social.

Remember that these games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook, so you should always make sure to read their terms of service and privacy policies to understand how they treat your data.

Controlling what information you share with applications

When you connect with a game, application or website - such as by going to a game, logging in to a website using your Facebook account, or adding an app to your timeline - we give the game, application, or website (sometimes referred to as just "Applications" or "Apps") your basic info (we sometimes call this your "public profile"), which includes your User ID and your public information. We also give them your friends' User IDs (also called your friend list) as part of your basic info.

Your friend list helps the application make your experience more social because it lets you find your friends on that application. Your User ID helps the application personalize your experience because it can connect your account on that application with your Facebook account, and it can access your basic info, which includes your public information and friend list. This includes the information you choose to make public, as well as information that is always publicly available. If the application needs additional information, such as your stories, photos or likes, it will have to ask you for specific permission.

The "Apps you use" setting lets you control the applications you use. You can see the permissions you have given these applications, the last time an application accessed your information, and the audience on Facebook for timeline stories and activity the application posts on your behalf. You can also remove applications you no longer want, or turn off all Platform applications. When you turn all Platform applications off, your User ID is no longer given to applications, even when your friends use those applications. But you will no longer be able to use any games, applications or

websites through Facebook.

When you first visit an app, Facebook lets the app know your language, your country, and whether you are in an age group, for instance, under 18, between 18-20, or 21 and over. Age range lets apps provide you with age-appropriate content. If you install the app, it can access, store and update the information you've shared. Apps you've installed can update their records of your basic info, age range, language and country. If you haven't used an app in a while, it won't be able to continue to update the additional information you've given them permission to access. Learn more at: https://www.facebook.com/help/how-apps-work

Sometimes a game console, mobile phone, or other device might ask for permission to share specific information with the games and applications you use on that device. If you say okay, those applications will not be able to access any other information about you without asking specific permission from you or your friends.

Sites and apps that use Instant Personalization receive your User ID and friend list when you visit them.

You always can remove apps you've installed by using your app settings at: https://www.facebook.com/settings/?tab=applications. But remember, apps may still be able to access your information when the people you share with use them. And, if you've removed an application and want them to delete the information you've already shared with them, you should contact the application and ask them to delete it. Visit the application's page on Facebook or their own website to learn more about the app. For example, Apps may have reasons (e.g. legal obligations) to retain some data that you share with them.

Controlling what is shared when the people you share with use applications

Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use.

Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social. For example, one of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of that application, your friend would want to give the application her friend list – which includes your User ID – so the application knows which of her friends is also using it. Your friend might also want to share the music you "like" on Facebook. If you have made that information public, then the application can access it just like anyone else. But if you've shared your likes with just your friends, the application could ask your friend for permission to share them.

You can control most of the information other people can share with applications they use from the "Ads, Apps and Websites" settings page. But these controls do not let you limit access to your public information and friend list.

If you want to completely block applications from getting your information when your friends and others use them, you will need to turn off all Platform applications. This means that you will no longer be able to use any third-party Facebook-integrated games, applications or websites.

If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission and no one else.

Logging in to another site using Facebook

Facebook Platform lets you log into other applications and websites using your Facebook account. When you log in using Facebook, we give the site your User ID (just like when you connect with any other application), but we do not share your email address or password with that website through this process without your permission.

If you already have an account on that website, the site may also be able to connect that account with your Facebook account. Sometimes it does this using what is called an "email hash", which is similar to searching for someone on Facebook using an email address. Only the email addresses in this case are hashed so no email addresses are actually shared between Facebook and the website.

How it works

The website sends over a hashed version of your email address, and we match it with a database of email addresses that we have also hashed. If there is a match, then we tell the website the User ID associated with the email address. This way, when you log into the website using Facebook, the website can link your Facebook account to your account on that website.

About social plugins

Social plugins are buttons, boxes, and stories (such as the Like button) that other websites can use to present Facebook content to you and create more social and personal experiences for you. While you view these buttons, boxes, and stories on other sites, the content comes directly from Facebook.

Sometimes plugins act just like applications. You can spot one of these plugins because it will ask you for permission to access your information or to publish information back to Facebook. For example, if you use a registration plugin on a website, the plugin will ask your permission to share your basic info with the website to make it easier for you to register for the website. Similarly, if you use an Add To Timeline plugin, the plugin will ask your permission to publish stories about your activities on that website to Facebook.

If you make something public using a plugin, such as posting a public comment on a newspaper's website, then that website can access your comment (along with your User ID) just like everyone else.

If you post something using a social plugin and you do not see a sharing icon, you should assume that story is Public. For example, if you post a comment through a Facebook comment plugin on a site, your story is Public and everyone, including the website, can see your story.
Websites that use social plugins can sometimes tell that you have engaged with the social plugin. For example, they may know that you clicked on a Like button in a social plugin.
We receive data when you visit a site with a social plugin. We keep this data for a maximum of 90 days. After that, we remove your name or any other personally identifying information from the data, or combine it with other people's data in a way that it is no longer associated with you. Learn more at: https://www.facebook.com/help/social-plugins

About instant personalization

Instant personalization (sometimes also referred to as "Start now") is a way for Facebook to help partners (such as Bing and Rotten Tomatoes) on and off Facebook create a more personalized and social experience for logged in users than a social plugin can offer. When you visit a site or app using instant personalization, it will know some information about you and your friends the moment you arrive. This is because sites and apps using instant personalization can access your User ID, your friend list, and your public information.

The first time you visit a site or app using instant personalization, you will see a notification letting you know that the site or app has partnered with Facebook to provide a personalized experience.

The notification will give you the ability to disable or turn off instant personalization for that site or app. If you do that, that site or app is required to delete all of the information about you it received from Facebook as part of the instant personalization program. In addition, we will prevent that site from accessing your information in the future, even when your friends use that site.

If you decide that you do not want to experience instant personalization for all partner sites and apps, you can disable instant personalization from the “Ads, Apps and Websites” settings page.

If you turn off instant personalization, these partner third party sites and apps will not be able to access your public information, even when your friends visit those sites.

If you turn off an instant personalization site or app after you have been using it or visited it a few times (or after you have given it specific permission to access your data), it will not automatically delete information about you it received through Facebook. Like all other apps, the site is required by our policies to delete information about you if you ask it to.

How it works

To join the instant personalization program, a potential partner must enter into an agreement with us designed to protect your privacy. For example, this agreement requires that the partner delete information about you if you turn off instant personalization when you first visit the site or app. It also prevents the partner from accessing any information about you until you or your friends visit its site.

Instant personalization partners sometimes use an email hash process to see if any of their users are on Facebook and get those users' User IDs. This process is similar to searching for someone on Facebook using an email address, except in this case the email addresses are hashed so no actual email addresses are exchanged. The partner is also contractually required not to use your User ID for any purpose (other than associating it with your account) until you or your friends visit the site.

When you visit a site or app using instant personalization, we provide the site or app with your User ID and your friend list (as well as your age range, locale, and gender). The site or app can then connect your account with that partner with your friends' accounts to make the site or app instantly social. The site can also access public information associated with any of the User IDs it receives, which it can use to make them instantly personalized. For example, if the site is a music site, it can access your music interests to suggest songs you may like, and access your friends' music interests to let you know what they are listening to. Of course it can only access your or your friends' music interests if they are public. If the site or app wants any additional information, it will have to get your specific permission.

Public search engines

Your public search setting controls whether people who enter your name on a public search engine may see your public timeline (including in sponsored results). You can find your public search setting on the "Ads, Apps and Websites" settings page.

This setting does not apply to search engines that access your information as an application using Facebook Platform. If you turn your public search setting off and then search for yourself on a public search engine, you may still see a preview of your timeline. This is because some search engines cache information for a period of time. You can learn more about how to request a search engine to remove you from cached information at: https://www.facebook.com/help/?faq=13323

IV. How advertising and Sponsored Stories work

Personalized ads

We do not share any of your information with advertisers (unless, of course, you give us permission). As described in this policy, we may share your information when we have removed from it anything that personally identifies you or combined it with other information so that it no longer personally identifies you.

We use the information we receive, including the information you provide at registration or add to your account or timeline, to deliver ads and to make them more relevant to you. This includes all of the things you share and do on Facebook, such as the Pages you like or key words from your stories, and the things we infer from your use of Facebook. Learn more at: https://www.facebook.com/help/?page=226611954016283

When an advertiser creates an ad, they are given the opportunity to choose their audience by location, demographics, likes, keywords, and any other information we receive or can tell about you and other users. For example, an advertiser can choose to target 18 to 35 year-old women who live in the United States and like basketball. An advertiser could also choose to target certain topics or keywords, like "music" or even people who like a particular song or artist. If you indicate that you are interested in topics, such as by liking a Page, including topics such as products, brands, religion, health status, or political views, you may see ads related to those topics as well. We require advertisers to comply with our Advertising Guidelines, including provisions relating to the use of sensitive data. Try this tool yourself to see one of the ways advertisers target ads and what information they see at: https://www.facebook.com/ads/create/

If the advertiser chooses to run the ad (also known as placing the order), we serve the ad to people who meet the criteria the advertiser selected, but we do not tell the advertiser who any of those people are. So, for example, if a person views or otherwise interacts with the ad, the advertiser might infer that the person is an 18-to-35-year-old woman who lives in the U.S. and likes basketball. But we would not tell the advertiser who that person is.

After the ad runs, we provide advertisers with reports on how their ads performed. For example we give advertisers reports telling them how many users saw or clicked on their ads. But these reports are anonymous. We do not tell advertisers who saw or clicked on their ads.

Advertisers or their partners sometimes place cookies on your computer (or use other similar system technologies) in order to serve ads and to make their ads more effective. Learn more about cookies, pixels and other system technologies.

Sometimes we allow advertisers to target a category of user, like a "moviegoer" or a "sci-fi fan." We do this by bundling characteristics that we believe are related to the category. For example, if a person "likes" the "Star Trek" Page and mentions "Star Wars" when they check into a movie theater, we may conclude that this person is likely to be a sci-fi fan. Advertisers of sci-fi movies, for example, could ask us to target “sci-fi fans” and we would target that group, which may include you. Or if you “like” Pages that are car-related and mention a particular car brand in a post, we might put you in the “potential car buyer” category and let a car brand target to that group, which would include you.

Ads + social context

Facebook Ads are sometimes paired with social actions your friends have taken. For example, an ad for a sushi restaurant may be paired with a news story that one of your friends likes that restaurant's Facebook page.

This is the same type of news story that could show up in your News Feed, only we place it next to a paid advertisement to make that ad more relevant and interesting.

When you show up in one of these news stories, we will only pair it with ads shown to your friends. If you do not want to appear in stories paired with Facebook Ads, you can opt out using your “Edit social ads” setting.

Learn what happens when you click "Like" on an advertisement or an advertiser's Facebook Page at: https://www.facebook.com/help/?faq=19399

We may serve ads, including those with social context (or serve just social context), on other sites. These work just like the ads we serve on Facebook - the advertisers do not receive any of your information. Only people that could see the Facebook action (like on your timeline) would see it paired in this way.

Your “Show my social actions in Facebook Ads” setting only controls ads with social context. It does not control Sponsored Stories, ads or information about Facebook's services and features, or other Facebook content.

Games, applications and websites can serve ads directly to you or help us serve ads to you or others if they have information like your User ID or email address.

Sponsored stories

Many of the things you do on Facebook (like "liking" a Page) are posted to your timeline and shared in News Feed. But there's a lot to read in News Feed. That's why we allow people to "sponsor" your stories to make sure your friends and subscribers see them. For example, if you RSVP to an event hosted by a local restaurant, that restaurant may want to make sure your friends see it so they can come too.

If they do sponsor a story, that story will appear in the same place ads usually do or in your News Feed under the heading "Sponsored" or something similar. Only people that could originally see the story can see the sponsored story, and no personal information about you (or your friends) is shared with the sponsor.

Your “Show my social actions in Facebook Ads” setting only controls ads with social context. It does not control Sponsored Stories, ads or information about Facebook's services and features, or other Facebook content.

Facebook content

We like to tell you about some of the features and tools your friends and others use on Facebook, to help you have a better experience. For example, if your friend uses our friend finder tool to find more friends on Facebook, we may tell you about it to encourage you to use it as well. This of course means your friend may similarly see suggestions based on the things you do. But we will try to only show it to friends that could benefit from your experience.

Your “Show my social actions in Facebook Ads” setting only controls ads with social context. It does not control Sponsored Stories, ads or information about Facebook's services and features, or other Facebook content.

V. Cookies, pixels and other similar technologies

Cookies are small pieces of data that are stored on your computer, mobile phone or other device. Pixels are small blocks of code on webpages that do things like allow another server to measure viewing of a webpage and often are used in connection with cookies.

We use technologies like cookies, pixels, and local storage (like on your browser or device, which is similar to a cookie but holds more information) to provide and understand a range of products and services. Learn more at: https://www.facebook.com/help/cookies

We use these technologies to do things like:

- make Facebook easier or faster to use;
- enable features and store information about you (including on your device or in your browser cache) and your use of Facebook;
- deliver, understand and improve advertising;
- monitor and understand the use of our products and services; and
- to protect you, others and Facebook.

For example, we may use them to know you are logged in to Facebook, to help you use social plugins and share buttons, or to know when you are interacting with our advertising or Platform partners.

We may ask advertisers or other partners to serve ads or services to computers, mobile phones or other devices, which may use a cookie, pixel or other similar technology placed by Facebook or the third party (although we would not share any other information that identifies you with an advertiser).

Most companies on the web use cookies (or other similar technological tools), including our advertising and Platform partners. For example, our Platform partners, advertisers or Page administrators may use cookies or similar technologies when you access their apps, ads, Pages or other content.

Cookies and things like local storage help make Facebook work, like allowing pages to load faster because certain content is stored on your browser or by helping us authenticate you to deliver personalized content.
To learn more about how advertisers generally use cookies and the choices advertisers provide, visit the Network Advertising Initiative at http://www.networkadvertising.org/managing/opt_out.asp, the Digital Advertising Alliance at http://www.aboutads.info/, the Internet Advertising Bureau (US) at http://www.iab.net or the Internet Advertising Bureau (EU) at http://youronlinechoices.eu/.
Refer to your browser or device's help material to learn what controls you can often use to remove or block cookies or other similar technologies or block or remove other data stored on your computer or device (such as by using the various settings in your browser). If you do this, it may affect your ability to use Facebook or other websites and apps.

VI. Some other things you need to know

Safe harbor

Facebook complies with the U.S.-EU and U.S.-Swiss Safe Harbor frameworks as set forth by the Department of Commerce regarding the collection, use, and retention of data from the European Union. To view our certification, visit the U.S. Department of Commerce's Safe Harbor website at: https://safeharbor.export.gov/list.aspx. As part of our

participation in the Safe Harbor program, we agree to resolve disputes you have with us in connection with our policies and practices through TRUSTe. If you would like to contact TRUSTe, visit:https://feedback-form.truste.com/watchdog/request

Contact us with questions or disputes

If you have questions or complaints regarding our Data Use Policy or practices, please contact us by mail at 1601 Willow Road, Menlo Park, CA 94025 if you reside in the U.S. or Canada, or at Facebook Ireland Ltd., Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland if you live outside the U.S. or Canada. Anyone may also contact us through this help page: https://www.facebook.com/help/contact_us.php?id=173545232710000

Responding to legal requests and preventing harm

We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; and to prevent death or imminent bodily harm. Information we receive about you, including financial transaction data related to purchases made with Facebook Credits, may be accessed, processed and retained for an extended period of time when it is the subject of a legal request or obligation, governmental investigation, or investigations concerning possible violations of our terms or policies, or otherwise to prevent harm. We also may retain information from accounts disabled for violations of our terms for at least a year to prevent repeat abuse or other violations of our terms.

Access requests

You can access and correct most of your personal data stored by Facebook by logging into your account and viewing your timeline and activity log. You can also download a copy of your personal data by visiting your "Account Settings", clicking on "Download a copy of your Facebook data" and then clicking on the link for your expanded archive. Learn more at: https://www.facebook.com/help/?faq=226281544049399

Notifications and Other Messages

We may send you notifications and other messages using the contact information we have for you, like your email address. You can control most of the notifications you receive, including ones from Pages you like and applications you use, using controls we provide, such as a control included in the email you receive or in your "Notifications" settings.

Friend finder

We offer tools to help you upload your friends' contact information so that you and others can find friends on Facebook, and invite friends who do not use Facebook to join, and so we can offer you and others better experiences on Facebook through suggestions and other customized experiences. If you do not want us to store this information, visit this help page at: https://www.facebook.com/contact_importer/remove_uploads.php.

If you give us your password, we will delete it after you upload your friends' contact information.

Invitations

When you invite a friend to join Facebook, we send a message on your behalf using your name, and we may also include names and pictures of other people your friend might know on Facebook. We'll also send a few reminders to those you invite, but the invitation will also give your friend the opportunity to opt out of receiving other invitations to join Facebook.

Memorializing accounts

We may memorialize the account of a deceased person. When we memorialize an account, we keep the timeline on Facebook, but limit access and some features. You can report a deceased person's timeline at: https://www.facebook.com/help/contact.php?show_form=deceased

We also may close an account if we receive a formal request that satisfies certain criteria.

Affiliates

We may share information we receive with businesses that are legally part of the same group of companies that Facebook is part of, or that become part of that group (often these companies are called affiliates). Likewise, our affiliates may share information with us as well. This sharing is done in compliance with applicable laws including where such applicable laws require consent. We and our affiliates may use shared information to help provide, understand, and improve our services and their own services.

Service Providers

We give your information to the people and companies that help us provide, understand and improve the services we offer. For example, we may use outside vendors to help host our website, serve photos and videos, process payments, analyze data, conduct and publish research, measure the effectiveness of ads, or provide search results. In some cases we provide the service jointly with another company, such as the Facebook Marketplace. In all of these cases our partners must agree to only use your information consistent with the agreement we enter into with them, as well as this Data Use Policy.

Security and bugs

We do our best to keep your information secure, but we need your help. For more detailed information about staying safe on Facebook, visit the Facebook Security Page. We try to keep Facebook up, bug-free and safe, but can't make guarantees about any part of our services or products.

Change of Control

If the ownership of our business changes, we may transfer your information to the new owner so they can continue to operate the service. But they will still have to honor the commitments we have made in this Data Use Policy.

Notice of Changes

If we make changes to this Data Use Policy we will notify you (for example, by publication here and on the Facebook Site Governance Page). If the changes are material, we will provide you additional, prominent notice as appropriate under the circumstances. You can make sure that you receive notice directly by liking the Facebook Site Governance Page.

Opportunity to comment

Unless we make a change for legal or administrative reasons, or to correct an inaccurate statement, we will give you seven (7) days to provide us with comments on the change. After the comment period, if we adopt any changes, we will provide notice (for example, on the

EXHIBIT C

Date of Last Revision: January 30, 2015

We give you the power to share as part of our mission to make the world more open and connected. This policy describes what information we collect and how it is used and shared. You can find additional tools and information at Privacy Basics.

As you review our policy, keep in mind that it applies to all Facebook brands, products and services that do not have a separate privacy policy or that link to this policy, which we call the "Facebook Services" or "Services."

I. What kinds of information do we collect?

Depending on which Services you use, we collect different kinds of information from or about you.

- **Things you do and information you provide.** We collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include information in or about the content you provide, such as the location of a photo or the date a file was created. We also collect information about how you use our Services, such as the types of content you view or engage with or the frequency and duration of your activities.
- **Things others do and information they provide.** We also collect content and information that other people provide when they use our Services, including information about you, such as when they share a photo of you, send a message to you, or upload, sync or import your contact information.
- **Your networks and connections.** We collect information about the people and groups you are connected to and how you interact with them, such as the people you communicate with the most or the groups you like to share with. We also collect contact information you provide if you upload, sync or import this information (such as an address book) from a device.
- **Information about payments.** If you use our Services for purchases or financial transactions (like when you buy something on Facebook, make a purchase in a game, or make a donation), we collect information about the purchase or transaction. This includes your payment information, such as your credit or debit card number and other card information, and other account and authentication information, as well as billing, shipping and contact details.
- **Device information.** We collect information from or about the computers, phones, or other devices where you install or access our Services, depending on the permissions you've granted. We may associate the information we collect from your different devices, which helps us provide consistent Services across your devices. Here are some examples of the information we collect:
  - Attributes such as the operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers.
  - Device locations, including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals.
  - Connection information such as the name of your mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address.
- **Information from websites and apps that use our Services.** We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us.
- **Information from third-party partners.** We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.
- **Facebook companies.** We receive information about you from companies that are owned or operated by Facebook, in accordance with their terms and policies. Learn more about these companies and their privacy policies.

II. How do we use this information?

We are passionate about creating engaging and customized experiences for people. We use all of the information we have to help us provide and support our Services. Here's how:

- **Provide, improve and develop Services.** We are able to deliver our Services, personalize content, and make suggestions for you by using this information to understand how you use and interact with our Services and the people or things you're connected to and interested in on and off our Services.

  We also use information we have to provide shortcuts and suggestions to you. For example, we are able to suggest that your friend tag you in a picture by comparing your friend's pictures to information we've put together from your profile pictures and the other photos in which you've been tagged. If this feature is enabled for you, you can control whether we suggest that another user tag you in a photo using the "Timeline and Tagging" settings.

  When we have location information, we use it to tailor our Services for you and others, like helping you to check-in and find local events or offers in your area or tell your friends that you are nearby.

  We conduct surveys and research, test features in development, and analyze the information we have to evaluate and improve products and services, develop new products or features, and conduct audits and troubleshooting activities.

- **Communicate with you.** We use your information to send you marketing communications, communicate with you about our Services and let you know about our policies and terms. We also use your information to respond to you when you contact us.
- **Show and measure ads and services.** We use the information we have to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services. Learn more about advertising on our Services and how you can control how information about you is used to personalize the ads you see.
- **Promote safety and security.** We use the information we have to help verify accounts and activity, and to promote safety and security on and off of our Services, such as by investigating suspicious activity or violations of our terms or policies. We work hard to protect your account using teams of engineers, automated systems, and advanced technology such as encryption and machine learning. We also offer easy-to-use security tools that add an extra layer of security to your account. For more information about promoting safety on Facebook, visit the Facebook Security Help Center.

We use cookies and similar technologies to provide and support our Services and each of the uses outlined and described in this section of our policy. Read our Cookie Policy to learn more.

III. How is this information shared?

Sharing On Our Services

People use our Services to connect and share with others. We make this possible by sharing your information in the following ways:

- **People you share and communicate with.**

  When you share and communicate using our Services, you choose the audience who can see what you share. For example, when you post on Facebook, you select the audience for the post, such as a customized group of individuals, all of your Friends, or members of a Group. Likewise, when you use Messenger, you also choose the people you send photos to or message.

  Public information is any information you share with a public audience, as well as information in your Public Profile, or content you share on a Facebook Page or another public forum. Public information is available to anyone on or off our Services and can be seen or accessed through online search engines, APIs, and offline media, such as on TV.

In some cases, people you share and communicate with may download or re-share this content with others on and off our Services. When you comment on another person's post or like their content on Facebook, that person decides the audience who can see your comment or like. If their audience is public, your comment will also be public.

- **People that see content others share about you.** Other people may use our Services to share content about you with the audience they choose. For example, people may share a photo of you, mention or tag you at a location in a post, or share information about you that you shared with them. If you have concerns with someone's post, social reporting is a way for people to quickly and easily ask for help from someone they trust. Learn More.

- **Apps, websites and third-party integrations on or using our Services.** When you use third-party apps, websites or other services that use, or are integrated with, our Services, they may receive information about what you post or share. For example, when you play a game with your Facebook friends or use the Facebook Comment or Share button on a website, the game developer or website may get information about your activities in the game or receive a comment or link that you share from their website on Facebook. In addition, when you download or use such third-party services, they can access your Public Profile, which includes your username or user ID, your age range and country/language, your list of friends, as well as any information that you share with them. Information collected by these apps, websites or integrated services is subject to their own terms and policies.

  Learn more about how you can control the information about you that you or others share with these apps and websites.

- **Sharing within Facebook companies.** We share information we have about you within the family of companies that are part of Facebook. Learn more about our companies.
- **New owner.** If the ownership or control of all or part of our Services or their assets changes, we may transfer your information to the new owner.

Sharing With Third-Party Partners and Customers

We work with third party companies who help us provide and improve our Services or who use advertising or related products, which makes it possible to operate our companies and provide free services to people around the world.

Here are the types of third parties we can share information with about you:

- **Advertising, Measurement and Analytics Services (Non-Personally Identifiable Information Only).** We want our advertising to be as relevant and interesting as the other information you find on our Services. With this in mind, we use all of the information we have about you to show you relevant ads. We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you. For example, we may tell an advertiser how its ads performed, or how many people viewed their ads or installed an app after seeing an ad, or provide non-personally identifying demographic information (such as 25 year old female, in Madrid, who likes software engineering) to these partners to help them understand their audience or customers, but only after the advertiser has agreed to abide by our advertiser guidelines.

  Please review your advertising preferences to understand why you're seeing a particular ad on Facebook. You can adjust your ad preferences if you want to control and manage your ad experience on Facebook.

- **Vendors, service providers and other partners.** We transfer information to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys. These partners must adhere to strict

confidentiality obligations in a way that is consistent with this Data Policy and the agreements we enter into with them.

IV. How can I manage or delete information about me?

You can manage the content and information you share when you use Facebook through the Activity Log tool. You can also download information associated with your Facebook account through our Download Your Information tool.

We store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services.

You can delete your account any time. When you delete your account, we delete things you have posted, such as your photos and status updates. If you do not want to delete your account, but want to temporarily stop using Facebook, you may deactivate your account instead. To learn more about deactivating or deleting your account, click here. Keep in mind that information that others have shared about you is not part of your account and will not be deleted when you delete your account.

V. How do we respond to legal requests or prevent harm?

We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; or to prevent death or imminent bodily harm. For example, we may provide information to third-party partners about the reliability of your account to prevent fraud and abuse on and off of our Services. Information we receive about you, including financial transaction data related to purchases made with Facebook, may be accessed, processed and retained for an extended period of time when it is the subject of a legal request or obligation, governmental investigation, or investigations concerning possible violations of our terms or policies, or otherwise to prevent harm. We also may retain information from accounts disabled for violations of our terms for at least a year to prevent repeat abuse or other violations of our terms.

VI. How our global services operate

Facebook, Inc. complies with the US-EU and US-Swiss Safe Harbor framework for the collection, use and retention of information from the European Union and Switzerland, as set out by the Department of Commerce. To view our certification, visit the Safe Harbor website.

As part of our participation in the Safe Harbor program, we will resolve disputes you have with us in connection with our policies and practices through TRUSTe. You can contact TRUSTe through their website.

Facebook may share information internally within our family of companies or with third parties for purposes described in this policy. Information collected within the European Economic Area (“EEA”) may, for example, be transferred to countries outside of the EEA for the purposes as described in this policy.

VII. How will we notify you of changes to this policy?

We’ll notify you before we make changes to this policy and give you the opportunity to review and comment on the revised policy before continuing to use our Services.

VIII. How to contact Facebook with questions

To learn more about how privacy works on Facebook, please check out Privacy Basics.

If you have questions about this policy, here's how you can reach us:

If you live in the US or Canada…

Please contact Facebook, Inc. online or by mail at:

Facebook, Inc.
1601 Willow Road
Menlo Park, CA 94025

If you live anywhere else…

The data controller responsible for your information is Facebook Ireland Ltd., which you can contact online or by mail at:

Facebook Ireland Ltd.
4 Grand Canal Square, Grand Canal Harbour
Dublin 2, Ireland

EXHIBIT D

Platform Policy

1. Build a quality product
2. Give people control
3. Protect data
4. Encourage proper use
5. Follow the law
6. Things you should know

If you use these features, follow these additional policies:

7. Login
8. Ads
9. Games
10. Payments
11. App Center
12. Open Graph
13. Social Plugins
14. Marketing API
15. Pages API and Features
16. Messenger Platform
17. Messenger Expressions
18. Account Kit
19. Live API
20. Profile Expression Kit
21. Camera Platform
22. CrowdTangle API
23. Jobs Platform

24. Commerce Platform

25. Instant Experiences

Definitions

Last updated March 14, 2018

Facebook Platform Policy

1. Build a quality product

1. Build an app that is stable and easily navigable. Be sure your app insights reflect a positive experience.
2. Ensure that your app's content (including ads and user-generated content) meets our Community Standards.
3. Follow our Advertising Policies for your app name, icons, and description.
4. Keep your app or bot's description and categorization up-to-date.
5. Don't include promotional content in your app's icon (ex: don't overlay your icon image with "new", "sale", "update" or any type of notification jewel).
6. Don't confuse, deceive, defraud, mislead, spam or surprise anyone.
7. Keep your app's negative feedback below our thresholds.
8. Follow any instructions we include in our technical documentation.

2. Give people control

1. Obtain consent from people before publishing content on their behalf.

2. Use publishing permissions to help people share on Facebook, not to send people messages from your app.

3. Don't prefill captions, comments, messages, or the user message parameter of posts with content a person or business didn't create, even if the person can edit or remove the content before sharing. You may use our Share Dialogs to prefill a single hashtag in a post, but don't prefill any content a person or business didn't create via the API.

4. Provide a publicly available and easily accessible privacy policy that explains what data you are collecting and how you will use that data.

5. You may use Account Information in accordance with your privacy policy and other Facebook policies. All other data may only be used outside your app after you have obtained explicit user consent.

6. Include your privacy policy URL in the App Dashboard.

7. Link to your privacy policy in any app store that allows you to.

8. Comply with your privacy policy.

9. Delete all of a person's data you have received from us (including friend data) if that person asks you to, unless you are required to keep it by law, regulation, or separate agreement with us. You may keep aggregated data only if no information identifying a specific person could be inferred or created from it.

10. Obtain consent from people before using their data in any ad.

11. Obtain adequate consent from people before using any Facebook technology that allows us to collect and process data about them, including for example, our SDKs and browser pixels. When you use such technology, provide an appropriate disclosure:

    a. That third parties, including Facebook, may use cookies, web beacons, and other storage technologies to collect or receive information from your websites, apps and elsewhere on the internet and use that information to provide measurement services, target ads and as described in our Data Policy; and

    b. How users can opt-out of the collection and use of information for ad targeting and where a user can access a mechanism for exercising such choice.

12. In jurisdictions that require informed consent for the storing and accessing of cookies or other information on an end user's device (such as the European Union), ensure, in a verifiable manner, that an end user provides the necessary consent before you use Facebook technologies that enable us to store and access cookies or other information on the end user's device. For suggestions on implementing consent mechanisms, visit Facebook's Cookie Consent Guide for Sites and Apps.

13. Obtain consent from people before you give us information that you independently collected from them.

14. Provide meaningful customer support for your app, and make it easy for people to contact you.

15. If people come to your app from the Facebook app on iOS, give them an option to go back to the Facebook app by using the Back to Facebook banner provided in our SDK.

16. If people come to your app from the Facebook app on Android, don't prevent them from going back to Facebook when they press the system back button.

3. Protect data

1. Protect the information you receive from us against unauthorized access, use, or disclosure. For example, don't use data obtained from us to provide tools that are used for surveillance.

2. Only show data obtained from a user access token on the devices associated with that token.

3. Only use friend data (including friends list) in the person's experience in your app.

4. If you cache data you receive from us, use it to improve your app's user experience and keep it up to date.

5. Don't proxy, request or collect Facebook usernames or passwords.

6. Keep private your secret key and access tokens. You can share them with an agent acting to operate your app if they sign a confidentiality agreement.

7. If you use any partner services, make them sign a contract to protect any information you obtained from us, limit their use of that information, and keep it confidential.

8. Keep Facebook user IDs within your control. Contract with any providers who help you build or run your app to ensure that they keep the user IDs secure and confidential and comply with our policies. If you need an anonymous unique identifier to share with third parties, use our mechanism.

9. Don't sell, license, or purchase any data obtained from us or our services.

10. Don't transfer any data that you receive from us (including anonymous, aggregate, or derived data) to any ad network, data broker or other advertising or monetization-related service.

11. Don't put Facebook data in a search engine or directory, or include web search functionality on Facebook.

12. If you are acquired by or merge with a third party, you can continue to use our data only within your app.

13. If you stop using Platform, promptly delete all user data you have received from us (absent explicit consent from people). You can keep Account Information if you have presented your privacy policy within your app.

14. If you use friend data from Facebook to establish social connections in your app, only do so if each person in that connection has granted you access to that information.

15. Don't use data obtained from Facebook to make decisions about eligibility, including whether to approve or reject an application or how much interest to charge on a loan.

4. Encourage proper use

1. Add something unique to the community. Don't replicate core functionality that Facebook already provides.

2. Respect the way Facebook looks and functions. Don't offer experiences that change it.

3. If you're building an app with a personalized or social experience, enable people to easily share on Facebook content they've created.

4. Respect the limits we've placed on Facebook functionality.

5. Only incentivize a person to log into your app, enter a promotion on your app's Page, check-in at a place, or to use Messenger to communicate with your business. Don't incentivize other actions.

6. Encourage people to accurately tag and share content.

7. If your service integrates a person's data into a physical product, only create a physical product for that person's personal and non-commercial use.

8. Don't build an app whose primary purpose is to redirect people off of Facebook.

9. If you want to use our logos or brand, follow the guidelines in the Facebook Brand Resource and Permissions Center and Brand Guidelines for Facebook Developers. Ad networks and data brokers must get our written permission before using our Platform, logos, or trademarks.

10. Don't sell, transfer or sublicense our code, APIs, or tools to anyone.

11. Only use our SDKs to develop and distribute apps or content for use with the Facebook Platform. You may also distribute any object code or sample source code included in the SDKs for inclusion in such apps.

12. Don’t modify, translate, create derivative works of, or reverse engineer any SDK or its components.

13. Be honest about your relationship with Facebook when talking to the press or users. Comply with our Developer PR Guidelines and get approval from us before issuing any formal press release or blog post mentioning Facebook.

14. If you use the Like button on iOS or Android, don’t collect or use any information from it.

5. Follow the law

1. You are responsible for restricting access to your content in accordance with all applicable laws and regulations, including geo-filtering or age-gating access where required.

2. Don’t provide or promote content that infringes upon the rights of any third party.

3. Ensure that you own or secure all rights necessary to display, distribute and deliver all content in your app.

4. Satisfy all licensing, reporting and payout obligations to third parties in connection with your app.

5. If your app contains content submitted or provided by third parties:

a. In the United States, you must take all steps required to fall within the applicable safe harbors of the Digital Millennium Copyright Act including designating an agent to receive notices of claimed infringement, instituting a repeat infringer termination policy and implementing a notice and takedown process.

b. In other countries, you must comply with local copyright laws and implement an appropriate notice and takedown process for when you receive a notice of claimed infringement.

6. Don't knowingly share information with us that you have collected from children under the age of 13.

7. Web sites or services directed to children under 13: If you use Social Plugins or our JavaScript SDK for Facebook on sites and services that are directed to children under 13, you are responsible for complying with all applicable laws. For example, if your web site or service is directed to children in the United States, or knowingly collects personal information from children in the United States, you must comply with the U.S. Children's Online Privacy Protection Act. You must also adhere to our usage notes.

8. Comply with all applicable laws and regulations in the jurisdiction where your app is available. Do not expose Facebook or people who use Facebook to harm or legal liability as determined by us in our sole discretion.

9. If applicable, comply with the Video Privacy Protection Act (VPPA) and obtain any opt-in consent necessary to share data on Facebook.

10. You agree to indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs)

related to any claim against us related to your service, actions, content or information.

6. Things you should know

1. We can analyze your app, website, content, and data for any purpose, including commercial.

2. We can monitor or collect data related to your use of SDKs.

3. We will use information we receive from you or in connection with your Platform integration in accordance with our Data Policy.

4. You give us all rights necessary to enable your app to work with Facebook, including the right to incorporate information you provide to us into other parts of Facebook, and the right to attribute the source of information using your name or logos.

5. We may share your contact info with people who want to contact you.

6. We may use your name, logos, content, and information, including screenshots and video captures of your app, to demonstrate or feature your use of Facebook, worldwide and royalty-free.

7. You give us the right to link to or frame your app, and place content, including ads, around your app. If you use our social plugins, feed dialog or share button, you also give us permission to use and allow others to use such links and content on Facebook.

8. We can audit your app to ensure it is safe and does not violate our Terms. If requested, you must provide

us with proof that your app complies with our terms.

9. We can create apps or products that offer features and services similar to your app.

10. We don't guarantee that Platform will always be free.

11. If you exceed 5M MAU, 100M API calls per day, or 50M impressions per day, you may be subject to additional terms.

12. Facebook and its licensors reserve all right, title and interest, including all intellectual property and other proprietary rights, in and to all SDKs.

13. Any SDKs you receive from us are provided to you on an "as is" basis, without warranty of any kind.

14. We can issue a press release describing our relationship with you.

15. We may enforce against your app or web site if we conclude that your app violates our terms or is negatively impacting the Platform. We may or may not notify you in advance.

16. Enforcement is both automated and manual, and can include disabling your app, restricting you and your app's access to platform functionality, requiring that you delete data, terminating our agreements with you or any other action that we deem appropriate.

17. We communicate with developers through Developer Alerts and email from the fb.com or facebookmail.com domain. Ensure that the email address associated with your Facebook account and the email address registered to the app are current and that you don't filter out these messages.

18. We may change these terms at any time without prior notice. Please check them regularly. Your continued use of Platform constitutes acceptance of those changes.

19. Your use of Facebook technology is subject to this Platform Policy, our Statement of Rights and Responsibilities and any other terms that apply to the applicable technology.

7. Login

1. Verify that you have integrated Login correctly. Your app shouldn't crash or hang during the testing process.

2. Native iOS and Android apps that implement Facebook Login must use our official SDKs for login.

3. Use a clearly branded log in button that follows the guidelines in the Facebook Brand Resource Center.

4. Request only the data and publishing permissions your app needs.

5. If a person declines a permission, you can prompt them again after they indicate an intent to grant you the permission.

6. Provide a "Log Out" option that functions properly and is easy to find.

8. Ads

1. If you have ads in your app on Facebook, comply with our Advertising Policies.

2. Avoid excessive ads. Don't let ads distract from your app's functionality.

3. Don't include ads in Page Tab apps.

4. If you use a third party ad provider to include ads in your app on Facebook, only use a provider from this list.

5. Don't include third-party ads (including for other apps) in posts, comments, notifications, requests, invites or messages.

6. Don't include or pair Platform Integrations with non-Facebook ads.

7. If you run a promotion, contest, competition, or sweepstake on Facebook, comply with our Promotions Policies.

9. Games

1. Games on Facebook.com:

   a. Don't share the same app ID with a desktop web game off of Facebook.com.

   b. Don't use your Facebook.com game or email addresses you've obtained from us to promote or link to a desktop web game off of Facebook.

   c. Use Facebook Payments as your only payment method for all in-game purchases.

d. Use Facebook Payments offers if you reward people for actions involving third parties.

2. Desktop web games off Facebook.com:

   a. Only use Facebook Login, social plugins, and publishing channels. Don't use connections such as friends lists.

   b. During authentication, only request age, email, and publishing permissions.

3. Games on mobile:

   a. Don't share the same app ID with a desktop web game off of Facebook.com.

   b. Don't use your mobile game or email addresses you've obtained from us to promote or link to a web game off of Facebook.

4. Instant Games:

   a. Don't charge for any items within your game. Games must be free to play.

   b. If you want to include ads within your game, only use the Games Ads API. Don't use a third party ad provider or include any other links to content off your game.

   c. Don't build, append to, edit, influence, or augment user profiles, including profiles associated with any mobile device identifier or other unique identifier that identifies any particular user, browser, computer or device.

   d. Don't post more than one Context Update per gameplay, without our prior permission.

5. If you want to facilitate or promote online gambling, online real money games of skill, or online lotteries, get our written permission before using any of our products.

6. If your game includes mandatory or optional in-app charges, explain this in your app's description.

10. Payments

1. If you use Facebook Payments, comply with the Facebook Developer Payments Terms.

2. Don't use Facebook Payments to solicit, collect or transfer funds for charitable causes without our prior permission.

3. If you're using iOS to run your app, use an iOS approved payment method.

4. If you accept payments on Facebook, only do so in your app.

11. App Center

1. Apps eligible for Facebook App Center must be games that use Facebook Login or games on Facebook.com.

2. App Detail and Description:

   a. Ensure the app's name and information are grammatically correct.

b. Ensure the app's language matches the App Center locale.

c. Don't include URLs or use the Facebook brand.

d. Don't include keyword lists, excessive punctuation, or non-standard symbols.

3. All Images:

   a. Use high quality, relevant images that reflect the app experience.

   b. Keep any image text concise. Don't obstruct images with text.

   c. Don't include ads, URLs or gimmicks such as Play buttons.

4. Icons:

   a. Use a transparent or colored background. If your icon requires a white background, use a colored border.

   b. If your logo has a drop shadow, use a colored background.

5. Banners:

   a. Don't include rounded edges or borders.

   b. Don't include third party logos.

6. Videos:

   a. Display the app's name.

   b. Clearly represent the purpose of the app and show accurate, relevant in-app experiences.

c. Keep your video high-quality and high-resolution.

d. Your video and its video cover image should be clear and recognizable. Don't include ads.

12. Open Graph

1. Open Graph Custom Actions:

   a. Don’t recreate actions that are already supported.

   b. Write the action and object in a clear and simple way.

   c. Make sure the story is grammatically correct.

   d. Use English for your submission.

   e. Don’t indicate a person’s consumption, browsing, discovering, or viewing of content.

   f. Don’t indicate a person has installed, visited, or connected to your app.

2. Read and Watch Actions:

   a. Publish actions only after a person has been on a page for more than 10 seconds.

   b. Allow people to remove stories published to Facebook on the same page where the content is hosted.

13. Social Plugins

1. Don’t include or pair Platform Integrations with non-Facebook advertisements.

2. Don’t sell or purchase placement of social plugins or sharer.php.

3. Don’t participate in any “like” or “share” exchange programs.

4. Don’t obscure or cover elements of social plugins.

5. Additional policies for the Quotes Plugin:

   a. Don't prefill quotes with content a person didn’t select, even if the person can edit or remove the content before sharing.

   b. The quotes plugin is intended to help people select their own quote to share. Use the app-defined quotes parameter if you want to suggest quotes for people to share.

   c. If you use the app-defined quotes parameter, the suggested quote must not contain URLs, ads, third party branded content or any other promotional content of any kind.

   d. Game apps must not use the quotes plugin.

14. Marketing API

1. Basic and Standard Ads API access may be downgraded to Development access after 30 days of non-use.

2. Don't use the Ads API if you're an ad network or data broker.

3. Don't promote content, services, or activities contrary to our competitive position, interests, or advertising philosophy.

4. Don't provide Partner Category targeting options that differ from those offered by Facebook.

5. Don't combine multiple end-advertisers or their Facebook connections (i.e. Pages) in the same ad account.

6. Free or trial versions of an ads API app:

   a. Don't allow more than 50 ad creations a day per customer.

   b. Require phone or email verification on new accounts.

   c. Don't allow affiliate networks to use your technology.

7. Pricing transparency:

   a. Only charge fees for the use of your tools and managed services with a fixed fee or variable percentage of ad spend.

   b. Proactively disclose to end advertisers the amount that you spent on Facebook advertising, using Facebook metrics (e.g., CPC, CPM rate), separate from your fees.

   c. Disclose the amount you charged as fees on Facebook advertising.

   d. We may disclose fees or the amount you spent on Facebook advertising to your clients if they request it.

e. We may require documentation from you to ensure your compliance with these terms.

f. Don't sell ads on a fixed CPM or CPC basis when using the Facebook advertising auction.

8. Data Collection and Use:

   a. If you have Standard Ads API access and our prior written permission, you can place 1x1 pixel view tags on advertisements.

   b. Ensure that any data that is collected is anonymous.

   c. Only use data from an end-advertiser's campaign to optimize or measure the performance of that end-advertiser's Facebook campaign.

   d. Don't use data to retarget on or off of Facebook.

   e. Don't mix data obtained from us with advertising campaigns on different platforms (without our written permission).

   f. Don't use data to build or augment any user profiles.

   g. Don't use piggybacking or redirects.

   h. Don't let people other than those acting on an end-advertiser's behalf access Facebook ad statistics.

9. Implement all bidding types including Optimized CPM.

10. Custom Audiences:

    a. If you use custom audiences, comply with the Custom Audience Terms.

b. Only use a client's data when creating custom audiences on their behalf.

c. Only use a Facebook User ID to create custom audiences when the person whose User ID is being used has logged into the client's app and has given the necessary consent.

d. Don't sell or transfer custom audiences.

11. Revoke an end-advertiser's access to your app if we request it.

12. Lead Ads:

    a. Only use a client's Lead Ads Data on behalf of that client.

    b. Don't combine Lead Ads Data from one client with Lead Ads Data from another client.

13. Ensure that people agree to Facebook's Statement of Rights and Responsibilities, including the Advertising Policies.

15. Pages API and Features

1. Pages API

    a. Don't charge a fee for creating, claiming, or managing a Page.

    b. Before enabling people to create a Page, first provide a means for them to claim an existing Place to prevent Page duplication.

    c. Ensure that people agree to Facebook's Statement of Rights and Responsibilities, including

the Advertising Policies.

d. Don't create or claim a Page on behalf of people without their consent.

e. Don't prevent people from gaining access to any Page you create or manage on their behalf.

f. Don't disclose administrators of a Page to third parties without the administrator's consent.

2. Pages Features: For all Platform features (ex: APIs) you use in connection with Pages, comply with the following:

a. Don’t charge a fee for using the Platform feature (or related Facebook Services). This policy does not prohibit you from charging for any of your other products and services unrelated to use of the Platform feature (or related Facebook Services).

b. Ensure that your agreement with the Page entity does not conflict with, and don't facilitate or encourage violations of, these Platform Policies, the Statement of Rights and Responsibilitiesand, if applicable, the Instagram Terms of Use.

c. Don't publish to an entity's Page without their consent.

d. We may remove items you publish to an entity's Page in our sole discretion.

e. Ensure you have the authority to use the Platform feature (or related Facebook Services) on the entity's behalf.

f. Don’t combine multiple entities or their Facebook Pages in the same account.

g. Revoke an entity's access to the Platform feature (or related Facebook Services) if we request it.

h. You grant us and our affiliates a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any data, content, and other information made available by you or on your behalf in connection with the Platform feature. This license survives even if you stop using the Platform feature. You are responsible for obtaining the necessary rights from all applicable rights holders to grant this license. Any API made available by you or on your behalf in connection with the Platform feature is deemed part of your App.

i. Data Collection and Use: If you are using the Platform feature (or related Facebook Services) on an entity's behalf, comply with the following:

i.a. Only use an entity's data on behalf of the entity (i.e., only to provide services to that entity and not for your own business purposes).

i.b. Don’t use an entity's data to build or augment user profiles.

i.c. Don't use an entity's data to retarget on or off of Facebook, use piggybacking or redirects, or combine an entity's data with data from another entity.

i.d. Don’t let people other than those acting on an entity’s behalf (ex: its employees or service providers) access the entity's data.

i.e. Delete all of an entity’s data you have received from us if that entity asks you to or if you stop providing services for that entity, unless you are required to keep it by law, regulation, or separate agreement with us.

16. Messenger Platform

1. Follow any instructions we include in our technical documentation.

2. Ensure your bot is stable and functions properly.

3. User authentication and opt-out:

   a. Place any user authentication method in a clear and conspicuous location to ensure people consent to initiating message threads.

   b. Don't contact people in Messenger unless you, or the party to whom you are operating as a service provider, have the necessary consent to do so.

   c. Messenger Opt-out: respect all requests (either on Messenger or off) by people to block, discontinue, or otherwise opt-out of your using Messenger to communicate with them.

4. Messenger Plugins:

   a. Don't obscure, cover or hide elements of our plugins.

   b. Ensure the Checkbox plugin is placed in close proximity to the button (ex: "purchase", "submit", "confirm") that a person must click on prior to you sending a MessengerCheckboxUserConfirmation event (i.e., don't send the event until after a person clicks on the button or takes an equivalent affirmative action (ex: submit form)).

5. Service Providers:

   a. Ensure your agreements with businesses do not conflict with, and that businesses agree to,

Facebook's Statement of Rights and Responsibilities, including these Platform Policies.

b. Ensure you have the authority to act as agent for the business to which you're providing a service, and that your use of our Platform is strictly for the benefit of that business.

c. Don't facilitate or encourage any violations of our policies. For example, if you have permission to support businesses that are eligible for Subscriptions, ensure you don't provide Subscriptions to ineligible services (see details below).

d. Your app should not receive excessive negative feedback. Be sure your app insights reflect a positive experience.

6. Maintain a Facebook Page that provides customer support contact information, including your mailing address and one or more of the following: email address, web address, or telephone number.

7. Messages and Data:

    1. Acceptable message types:

        a. After people interact with your business or Bot: You may message people within 24 hours of a person's interaction with your business or Bot (ex: messaging your Bot or interacting with a Messenger plugin on your website). Except as permitted below, and until the next interaction, you may send one additional message after this 24 hour period in order to follow up on your conversation.

        b. Message Templates and Tags: Only approved message templates and tags may be sent outside of the 24 hour period. Don't use a

message template or tag for a purpose other than its intended purpose.

c. Subscription-based messaging:

i. Bots that primarily support the following use cases are eligible for subscription-based messaging, and these messages may be sent at any time provided people opt-in to receiving this content:

1. News: Bots that inform people about recent or important events or information in categories such as sports, finance, business, real estate, weather, traffic, politics, government, non-profit organizations, religion, celebrities and entertainment.

2. Personal trackers: Bots that enable people to receive and monitor information about themselves in categories such as fitness, health, wellness, and finance.

3. Productivity: Bots that enable people to manage their personal productivity with tasks such as managing calendar events, receiving reminders, and paying bills.

ii. Subscriptions messages may not be used for sending advertising, marketing, solicitations, or promotional content, even if a person opts-in to receiving this content (ex: daily deals, coupons and discount or sale announcements are not permitted).

2. Data: Don't use any data obtained from us about the people you reach in Messenger, other than the content of message threads, for any

purpose other than as reasonably necessary to support the message types you elect to use.

3. Healthcare: Don't use Messenger to facilitate direct conversations between people and healthcare providers or to send or collect any patient data obtained from healthcare providers.

4. Disclosures: Ensure that you provide all necessary disclosures to people using Messenger, such as any disclosures needed to indicate the sponsored or advertising nature of content you send.

5. Offers and Payments:

   a. Don't share or ask people to share individual payment card, financial account numbers or other cardholder data within messages.

   b. Don't include links to sites off Messenger where payment information is collected, without our prior permission.

   c. If you have permission to offer or complete sales of goods or services within Messenger, adhere to the Facebook Commerce Product Merchant Agreement.

   d. Don't use Messenger Platform to sell digital goods.

8. Things You Should Know:

   a. We may limit or remove your access to Messenger if you receive large amounts of negative feedback or violate our policies, as determined by us in our sole discretion.

17. Messenger Expression

1. General Policies

    1. Ensure you comply with all applicable Platform Policies.
    2. Follow our technical documentation.
    3. Follow our Brand Guidelines if you want to use our logos or brand.
    4. Don't obscure or cover selected content in the share sheet.
    5. Allow people to immediately select or create content without interruption. Don't disrupt them with other information before they share.
    6. Notify people up front before allowing them to engage with paid content.
    7. Don't include ads in content you send to Messenger.
    8. Your logo and app name may only appear in the space we provide.
    9. Don't use Messenger as an app invite channel. Facilitate real time conversations that inspire people to respond with content from your app.
    10. Don't charge for most of the content in your app. Ensure your app contains free shareable content.
    11. If you exceed 400K impressions per day, you may be subject to additional terms.

2. Additional Policies for Optimized and Featured Apps

    1. Your app must not replicate core Facebook features or functionality, and must not promote your other apps that do so.

    2. Your app must be free to install.

    3. If your paid content is available in multiple apps, ensure it is offered for Messenger at the lowest price available.

    4. If people come to your app from Messenger, ensure your app's primary share experience is to Messenger.

    5. Don't send unengaging or long form content. Ensure your app only sends unique user generated content or engaging aggregated content to Messenger. Facilitate real time conversations that inspire people to respond to Messenger with content from your app.

    6. Ensure your call-to-action links to the same app that generated the content.

    7. When linking to your app from Messenger, you can present people with paid content so long as free shareable content is clearly available on the landing page.

    8. Implement App Events in your app, including activateApp and purchase events if your app offers in-app purchases.

    9. Optimized and featured functionality, including the availability of calls-to-action on content and in-Messenger discovery, is made available within our sole discretion and can be removed at any time.

18. Account Kit

1. Don't obscure any elements of the Account Kit user interface, and don't modify any element except where expressly permitted by our technical documentation.

2. If people log in with email addresses or phone numbers, your use of that data is subject to your privacy policy and any applicable law or regulation.

3. If you exceed 100K SMSs per month, you may be subject to additional terms.

4. If a person that logged in with an email address or phone number deletes their account or requests that such account be deleted, ensure that you notify us via the delete API.

5. If we remove your access to the Account Kit service, you have 30 days to request any account data that people provided through the Account Kit service as well as any data you've stored with us through the Preferences API. We will provide you with this information unless otherwise prohibited by law.

19. Live API

1. Don’t build apps that enable publishers to simultaneously stream to Facebook and other online streaming services.

2. Don’t use the API to stream directly from a mobile phone or tablet camera to Facebook.

3. Ensure any pre-recorded content is clearly distinguishable from live content.

4. Don't use the API to publish looping videos; static, animated, or looping images; or to live-stream polls associated with unmoving or ambient broadcasts.

5. If you enable people to publish Live Video to Facebook, remind them of their obligation to not include third party ads in their video content and to clearly distinguish any pre-recorded content from live content.

20. Profile Expression Kit

1. Don’t include ads or commercial content, such as logos and watermarks, in profile photos or videos.

2. Don’t include slideshows in profile photos or videos.

3. Don’t encourage people to upload profile photos or videos that they aren’t depicted in.

4. Only apps that have a primary purpose of creating and editing photos or videos may use the Profile Expression Kit.

21. Camera Platform

1. Don't make any changes to your effect after it has been approved. If you want to make any changes to your effect you must submit a new or improved effect for our review.

2. Ensure you comply with the Camera Effects Platform Policies.

22. CrowdTangle API

1. Don't share your access credentials outside of your organization.

2. We may limit or remove your access to the API if your memory, data, or CPU usage is excessive, as determined by us in our sole discretion.

3. Don't have front-end widgets call our API directly. Front-end widgets should use cached data collected through the API.

4. Don't use data to build or augment any user profiles.

5. Display the CrowdTangle logo in any integration and note CrowdTangle in any public facing description or announcement of the integration.

23. Jobs Platform

1. Follow any instructions we include in our Jobs Platform technical documentation.

2. Comply with these Platform Policies, with particular attention to the Pages Features section of the Page API and Features policies.

3. Ensure you implement the Facebook Pixel in accordance with our technical documentation, and that your use of our Facebook Pixel is subject to and complies with our Terms For Conversion Tracking,

Custom Audiences From Your Website, and Custom Audiences From Your Mobile App.

4. Ensure that job listings and your use of the Jobs Platform (including your use of data received via a job listing) comply with our Pages Terms.

5. If your App displays job applications obtained from Facebook, ensure you display “Applied on Facebook” in connection with such job applications.

24. Commerce Platform

1. General Policies

   a. If you are offering or completing sales of goods or services within Facebook or Instagram, comply with the Merchant Agreement.

   b. Follow any instructions we include in our technical documentation.

   c. If you want to use the Checkout features of the Commerce Platform (ex: features that allow users to initiate payments on Facebook Services or Instagram Services), you will need additional permissions from us and you will be subject to additional terms.

   d. Your use of Instagram Services in connection with your Commerce Platform integration is subject to, and you agree to comply with, the Instagram Terms of Use, Instagram Platform Policy, and other applicable Instagram terms.

2. Service Providers: If you enable a business to offer or complete sales of goods or services within Facebook or Instagram through your Commerce Platform

integration, ensure you also comply with the following:

a. Ensure that your agreements with the businesses do not conflict with, and that businesses agree to, the Merchant Agreement and, as applicable, our Statement of Rights and Responsibilities and/or the Instagram Terms of Use.

b. Don't facilitate or encourage violations of our policies and the Merchant Agreement.

c. Ensure you have the authority to act as a service provider for the business to whom you're providing your Commerce Platform integration, and that your use of Facebook Platform or Instagram platform is strictly for the benefit of that business.

d. Don't combine multiple end-businesses or their Facebook or Instagram connections (ex: Pages) in the same account.

e. Obtain consent from the applicable administrator before publishing to their Page or other account surface.

f. Don't charge a fee for using your Commerce Platform integrations. This policy does not prohibit you from charging for any of your other products and services unrelated to your Commerce Platform integrations.

g. Revoke a business's access to your Commerce Platform integration if we request it.

h. Ensure you distribute our Commerce Platform plugins only under our terms (ex: Merchant Agreement) and not your own terms and policies.

i. Don't obscure or cover elements of our Commerce Platform plugins.

3. “Commerce Platform” includes (a) the APIs, plugins, code, protocols, specifications, documentation, and other technologies and services described in the shops API technical documentation, and (b) any APIs, SDKs, plugins, code, protocols, specifications, technology and services that enable you to access certain features, functions and/or services on Instagram Services to offer or complete sales of goods or services.

25. Instant Experiences

1. Follow any instructions we include in our Instant Experiences technical documentation.

2. Comply with these Platform Policies, with particular attention to the Pages Features section of the Page API and Features policies.

3. Ensure you implement the Facebook Pixel in accordance with our technical documentation, and that your use of our Facebook Pixel is subject to and complies with our Terms For Conversion Tracking, Custom Audiences From Your Website, and Custom Audiences From Your Mobile App.

4. If you are offering or completing sales of goods or services with an Instant Experience, comply with the Merchant Agreement. If you are enabling another entity to offer or complete sales of goods or services with an Instant Experience, you must ensure that the entity agrees to the Merchant Agreement; and the Statement of Rights and Responsibilities; and if applicable the Instagram Terms of Use.

5. If you are using Instant Experience payment features (ex: PaymentRequest API): (a) ensure that the payment amount requested accurately reflects the total price presented to the customer for the goods or services requested by the customer, (b) you must comply with the payments section of the Merchant Agreement; and (c) you may only use payment features in countries outside of the United States with our approval.

6. Instagram: If you use any Platform feature on the Instagram Service, such use on the Instagram Service is subject to theses Platform Policies and the Instagram Terms of Use. For clarity, the Platform integration and use of the Platform feature on Facebook is subject to these Platform Policies and the Statement of Rights and Responsibilities. If you use any Instagram APIs, such use is subject to the Instagram Platform Policy.

Definitions

1. “App” means any technical integration we have assigned an app identification number.

2. "Account Information" consists of: name, email, gender, birthday, current city and profile picture URL.

3. "Marketing API" includes all Graph APIs related to advertising, and all Real Time APIs related to advertising, including but not limited to: all Lead Ads Data coming through the Graph API or Real Time Updates.

4. “User data” means any data, including a person's content or information that you or third parties obtain from or through Facebook.

5. "SDK" means any object code, source code, or documentation you receive from us that helps you create apps or content for use with the Facebook Platform.

6. By "Facebook" or "Facebook Services" we mean the features and services we make available, including through (a) our website at www.facebook.com and any other Facebook branded or co-branded websites (including sub-domains, international versions, widgets, and mobile versions); (b) our Platform; (c) social plugins such as the Like button, the Share button and other similar offerings; and (d) other media, brands, products, services, software (such as a toolbar), devices, or networks now existing or later developed. Facebook reserves the right to designate, in its sole discretion, that certain of our brands, products, or services are governed by separate terms and not our SRR.

EXHIBIT E

Platform Policy

1. Build a quality product
2. Give people control
3. Protect data
4. Encourage proper use
5. Follow the law
6. Things you should know

If you use these features, follow these additional policies:

7. Login
8. Ads
9. Games
10. Payments
11. App Center
12. Open Graph
13. Social Plugins
14. Ads API
15. Messenger
16. Definitions

Last updated March 25, 2015

Facebook Platform Policy

Other Languages

1. Build a quality product

1. Build an app that is stable and easily navigable.
2. Ensure that your app's content (including ads and user-generated content) meets our Community Standards.
3. Follow our Advertising Guidelines for your app name, icons, and description.
4. Keep your app's description and categorization up-to-date.
5. Don't confuse, deceive, defraud, mislead, spam or surprise anyone.
6. Keep your app's negative feedback below our thresholds.
7. Follow any instructions we include in our technical documentation.

2. Give people control

1. Obtain consent from people before publishing content on their behalf.
2. Use publishing permissions to help people share on Facebook, not to send people messages from your app.
3. Don't prefill captions, comments, messages, or the user message parameter of posts with content a person didn't create, even if the person can edit or remove the content before sh
4. Provide a publicly available and easily accessible privacy policy that explains what data you are collecting and how you will use that data.
5. You may use Account Information in accordance with your privacy policy and other Facebook policies. All other data may only be used outside your app after you have obtained explicit user consent.
6. Include your privacy policy URL in the App Dashboard.
7. Link to your privacy policy in any app marketplace that allows you to.
8. Comply with your privacy policy.
9. Delete all of a person's data you have received from us (including friend data) if that person asks you to, unless you are required to keep it by law, regulation, or separate agreement with us. You may keep aggregated data only if no information

identifying a specific person could be inferred or created from it.

10. Obtain consent from people before using their data in any ad.

11. Obtain adequate consent from people before using any Facebook technology that allows us to collect and process data about them, including for example, our SDKs and browser pixels. When you use such technology, disclose to people in your privacy policy that you are enabling us to collect and process data about them.

12. Obtain consent from people before you give us information that you independently collected from them.

13. If you are tracking a person's activity, provide an opt-out from that tracking.

14. Provide meaningful customer support for your app, and make it easy for people to contact you.

15. If people come to your app from the Facebook app on iOS, give them an option to go back to the Facebook app by using the Back to Facebook banner provided in our SDK.

16. If people come to your app from the Facebook app on Android, don't prevent them from going back to Facebook when they press the system back button.

3. Protect data

1. Protect the information you receive from us against unauthorized access or use.

2. Only show data obtained from a user access token on the devices associated with that token.

3. Only use friend data (including friends list) in the person's experience in your app.

4. If you cache data you receive from us, use it to improve your app's user experience and keep it up to date.

5. Don't proxy, request or collect Facebook usernames or passwords.

6. Keep private your secret key and access tokens. You can share them with an agent acting to operate your app if they sign a confidentiality agreement.

7. If you use any partner services, make them sign a contract to protect any information you obtained from us, limit their use of that information, and keep it confidential.

8. Keep Facebook user IDs within your control. Contract with any providers who help you build or run your app to ensure that they keep the user IDs secure and confidential and comply with our policies. If you need an anonymous unique identifier to share with third parties, use our mechanism.

9. Don't sell, license, or purchase any data obtained from us or our services.

10. Don't transfer any data that you receive from us (including anonymous, aggregate, or derived data) to any ad network, data broker or other advertising or monetization-related service.

11. Don't put Facebook data in a search engine or directory, or include web search

functionality on Facebook.

12. If you are acquired by or merge with a third party, you can continue to use our data only within your app.

13. If you stop using Platform, promptly delete all user data you have received from us (absent explicit consent from people). You can keep Account Information if you have presented your privacy policy within your app.

14. If you use friend data from Facebook to establish social connections in your app, only do so if each person in that connection has granted you access to that information.

4. Encourage proper use

1. Add something unique to the community. Don't replicate core functionality that Facebook already provides.

2. Respect the way Facebook looks and functions. Don't offer experiences that change it.

3. If you're building an app with a personalized or social experience, enable people to easily share on Facebook content they've created.

4. Respect the limits we've placed on Facebook functionality.

5. Only incentivize a person to log into your app, enter a promotion on your app's Page, or check-in at a place. Don't incentivize other actions.

6. Encourage people to accurately tag and share content.

7. If your service integrates a person's data into a physical product, only create a physical product for that person's personal and non-commercial use.

8. Don't build an app whose primary purpose is to redirect people off of Facebook.

9. If you want to use our logos or brand, follow the guidelines in the Facebook Brand Resource and Permissions Center. Ad networks and data brokers must get our written permission before using our Platform, logos, or trademarks.

10. Don't sell, transfer or sublicense our code, APIs, or tools to anyone.

11. Only use our SDKs to develop and distribute apps for use with the Facebook Platform. You may also distr bute any code l braries or sample source code included in the SDKs for inclusion in such apps.

12. Don't modify, translate, create derivative works of, or reverse engineer any SDK or its components.

13. Be honest about your relationship with Facebook when ta king to the press or users. Comply with our Developer PR Guidelines and get approval from us before issuing any formal press release or blog post mentioning Facebook.

14. If you use the Like button on iOS or Android, don't collect or use any information from it.

5. Follow the law

1. You are respons ble for restricting access to your content in accordance with all applicable laws and regulations, including geo-filtering or age-gating access where required.

2. Don't provide or promote content that infringes upon the rights of any third party.

3. Ensure that you own or secure all rights necessary to display, distribute and deliver all content in your app.

4. Satisfy all licensing, reporting and payout obligations to third parties in connection with your app.

5. If your app contains content submitted or provided by third parties:

   a. In the United States, you must take all steps required to fall within the applicable safe harbors of the Digital Millennium Copyright Act including designating an agent to receive notices of claimed infringement, instituting a repeat infringer termination policy and implementing a notice and takedown process.

   b. In other countries, you must comply with local copyright laws and implement an appropriate notice and takedown process for when you receive a notice of claimed infringement.

6. Don't knowingly share information with us that you have collected from children under the age of 13.

7. Web sites or services directed to children under 13: If you use Social Plugins or our JavaScript SDK for Facebook on sites and services that are directed to children under 13, you are respons ble for complying with all applicable laws. For example, if your web site or service is directed to children in the United States, or knowingly collects personal information from children in the United States, you must comply with the U.S. Children's Online Privacy Protection Act. You must also adhere to our usage notes.

8. Comply with all applicable laws and regulations in the jurisdiction where your app is available. Do not expose Facebook or people who use Facebook to harm or legal liability as determined by us in our sole discretion.

9. If applicable, comply with the Video Privacy Protection Act (VPPA) and obtain any opt-in consent necessary to share data on Facebook.

10. You agree to indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to any claim against us related to your service, actions, content or information.

6. Things you should know

1. We can analyze your app, website, content, and data for any purpose, including commercial.

2. We can monitor or collect data related to your use of SDKs.

3. We will use information we receive from you or in connection with your Platform integration in accordance with our Data Policy.

4. You give us all rights necessary to enable your app to work with Facebook, including the right to incorporate information you provide to us into other parts of Facebook, and the right to attribute the source of information using your name or logos.

5. We may share your contact info with people who want to contact you.

6. We may use your name, logos, content, and information, including screenshots and video captures of your app, to demonstrate or feature your use of Facebook, worldwide and royalty-free.

7. You give us the right to link to or frame your app, and place content, including ads, around your app. If you use our social plugins, feed dialog or share button, you also give us permission to use and allow others to use such links and content on Facebook.

8. We can audit your app to ensure it is safe and does not violate our Terms. If requested, you must provide us with proof that your app complies with our terms.

9. We can create apps or products that offer features and services similar to your app.

10. We don't guarantee that Platform will always be free.

11. If you exceed 5M MAU, 100M API calls per day, or 50M impressions per day, you may be subject to additional terms.

12. Facebook and its licensors reserve all right, title and interest, including all intellectual property and other proprietary rights, in and to all SDKs.

13. Any SDKs you receive from us are provided to you on an "as is" basis, without warranty of any kind.

14. We can issue a press release describing our relationship with you.

15. We may enforce against your app or web site if we conclude that your app violates our terms or is negatively impacting the Platform. We may or may not notify you in advance.

16. Enforcement is both automated and manual, and can include disabling your app, restricting you and your app's access to platform functionality, requiring that you delete data, terminating our agreements with you or any other action that we deem appropriate.

17. We communicate with developers through Developer Alerts and email from the fb.com or facebookmail.com domain. Ensure that the email address associated with your Facebook account and the email address registered to the app are current and that you don't filter out these messages.

18. We may change these terms at any time without prior notice. Please check them regularly. Your continued use of Platform constitutes acceptance of those changes.

19. If you use Social Plugins, Facebook SDKs, or operate a Platform app or website, you must follow our Statement of Rights and Responsibilities and these additional rules unless you have our written permission to do otherwise.

7. Login

1. Verify that you have integrated Login correctly. Your app shouldn't crash or hang during the testing process.
2. Native iOS and Android apps that implement Facebook Login must use our official SDKs for login.
3. Use a clearly branded "Login with Facebook" button and follow the Facebook Brand Guidelines.
4. Request only the data and publishing permissions your app needs.
5. If a person declines a permission, you can prompt them again after they indicate an intent to grant you the permission.
6. Provide a "Log Out" option that functions properly and is easy to find.

8. Ads

1. If you have ads in your app on Facebook, comply with our Advertising Guidelines.
2. Avoid excessive ads. Don't let ads distract from your app's functionality.
3. Don't include ads in Page Tab apps.
4. If you use a third party ad provider to include ads in your app on Facebook, only use a provider from this list.
5. Don't include third-party ads (including for other apps) in posts, notifications, or requests.
6. Don't include or pair Platform Integrations with non-Facebook ads.
7. If you run a promotion, contest, competition, or sweepstake on Facebook, comply with our Promotions Policies.

9. Games

1. Games on Facebook.com:

   a. Don't share the same app ID with a desktop web game off of Facebook.com.

   b. Don't use your Facebook.com game or email addresses you've obtained from us to promote or link to a desktop web game off of Facebook.

   c. Use Facebook Payments as your only payment method for all in-game purchases.

   d. Use Facebook Payments offers if you reward people for actions involving third parties.

2. Desktop web games off Facebook.com:

   a. Only use Facebook Login, social plugins, and publishing channels. Don't use connections such as friends lists.

   b. During authentication, only request age, email, and publishing permissions.

3. Games on mobile:

   a. Don't share the same app ID with a desktop web game off of Facebook.com.

   b. Don't use your mobile game or email addresses you've obtained from us to promote or link to a web game off of Facebook.

4. If you want to facilitate or promote online gambling, online real money games of skill, or online lotteries, get our written permission before using any of our products.

5. If your game includes mandatory or optional in-app charges, explain this in your app's description.

10. Payments

1. If you use Facebook Payments, comply with the Facebook Developer Payments Terms.

2. Don't use Facebook Payments to solicit, collect or transfer funds for charitable causes without our prior permission.

3. If you're using iOS to run your app, use an iOS approved payment method.

4. If you accept payments on Facebook, only do so in your app.

11. App Center

1. Apps eligible for the Facebook App Center must use Facebook Login or have a Facebook Canvas or Page Tab app.

2. App Detail and Description:

   a. Ensure the app's name and information are grammatically correct.

   b. Ensure the app's language matches the App Center locale.

   c. Don't include URLs or use the Facebook brand.

   d. Don't include keyword lists, excessive punctuation, or non-standard symbols.

3. All Images:

   a. Use high quality, relevant images that reflect the app experience.

   b. Keep any image text concise. Don't obstruct images with text.

c. Don't include ads, URLs or gimmicks such as Play buttons.

4. Icons:

   a. Use a transparent or colored background. If your icon requires a white background, use a colored border.

   b. If your logo has a drop shadow, use a colored background.

5. Banners:

   a. Don't include rounded edges or borders.

   b. Don't include third party logos.

6. Videos:

   a. Display the app's name.

   b. Clearly represent the purpose of the app and show accurate, relevant in-app experiences.

   c. Keep your video high-quality and high-resolution.

   d. Your video and its video cover image should be clear and recognizable. Don't include ads.

12. Open Graph

1. Open Graph Custom Actions:

   a. Don't recreate actions that are already supported.

   b. Write the action and object in a clear and simple way.

   c. Make sure the story is grammatically correct.

   d. Use English for your submission.

   e. Don't indicate a person's consumption, browsing, discovering, or viewing of content.

   f. Don't indicate a person has installed, visited, or connected to your app.

2. Read and Watch Actions:

   a. Publish actions only after a person has been on a page for more than 10 seconds.

   b. Allow people to remove stories published to Facebook on the same page where the content is hosted.

13. Social Plugins

1. Don't include or pair Platform Integrations with non-Facebook advertisements.
2. Don't sell or purchase placement of social plugins or sharer.php.
3. Don't participate in any "like" or "share" exchange programs.
4. Don't obscure or cover elements of social plugins.

14. Ads API

1. Basic and Standard Ads API access may be downgraded to Development access after 30 days of non-use.
2. Don't use the Ads API if you're an ad network or data broker.
3. Don't promote content, services, or activities contrary to our competitive position, interests, or advertising philosophy.
4. Don't provide Partner Category targeting options that differ from those offered by Facebook.
5. Don't combine multiple end-advertisers or their Facebook connections (i.e. Pages) in the same ad account.
6. Free or trial versions of an ads API app:

   a. Don't allow more than 50 ad creations a day per customer.

   b. Require phone or email verification on new accounts.

   c. Don't allow affiliate networks to use your technology.

7. Pricing transparency:

   a. Only charge fees for the use of your tools and managed services with a fixed fee or variable percentage of ad spend.

   b. Proactively disclose to end advertisers the amount that you spent on Facebook advertising, using Facebook metrics (e.g., CPC, CPM rate), separate from your fees.

   c. Disclose the amount you charged as fees on Facebook advertising.

   d. We may disclose fees or the amount you spent on Facebook advertising to your clients if they request it.

   e. We may require documentation from you to ensure your compliance with these terms.

   f. Don't sell ads on a fixed CPM or CPC basis when using the Facebook advertising auction.

8. Data Collection and Use:

a. If you have Standard Ads API access and our prior written permission, you can place 1x1 pixel view tags on advertisements.

b. Ensure that any data that is collected is anonymous.

c. Only use data from an end-advertiser's campaign to optimize or measure the performance of that end-advertiser's Facebook campaign.

d. Don't use data to retarget on or off of Facebook.

e. Don't mix data obtained from us with advertising campaigns on different platforms.

f. Don't use data to build or augment any user profiles.

g. Don't use piggybacking or redirects.

h. Don't let people other than those acting on an end-advertiser's behalf access Facebook ad statistics.

9. Implement all bidding types including Optimized CPM.
10. Custom Audiences:

    a. If you use custom audiences, comply with the Custom Audience Terms.

    b. Only use a client's data when creating custom audiences on their behalf.

    c. Only use a Facebook User ID to create custom audiences when the person whose User ID is being used has logged into the client's app and has given the necessary consent.

    d. Don't sell or transfer custom audiences.

11. Revoke an end-advertiser's access to your app if we request it.

15. Messenger

1. General Policies
    1. Ensure you comply with all applicable Platform Policies.
    2. Follow our technical documentation.
    3. Follow our Brand Guidelines if you want to use our logos or brand.
    4. Don't obscure or cover selected content in the share sheet.
    5. Allow people to immediately select or create content without interruption. Don't disrupt them with other information before they share.
    6. Notify people up front before allowing them to engage with paid content.
    7. Don't include ads in content you send to Messenger.
    8. Your logo and app name may only appear in the space we provide.

9. Don't use Messenger as an app invite channel. Facilitate real time conversations that inspire people to respond with content from your app.
10. Don't charge for most of the content in your app. Ensure your app contains free shareable content.
11. If you exceed 400K impressions per day, you may be subject to additional terms.

2. Additional Policies for Optimized and Featured Apps
    1. Your app must not replicate core Facebook features or functionality, and must not promote your other apps that do so.
    2. Your app must be free to install.
    3. If your paid content is available in multiple apps, ensure it is offered for Messenger at the lowest price available.
    4. Ensure your app's primary share experience is to Messenger.
    5. Don't send unengaging or long form content. Ensure your app only sends unique user generated content or engaging aggregated content to Messenger. Facilitate real time conversations that inspire people to respond to Messenger with content from your app.
    6. Ensure your call-to-action links to the same app that generated the content.
    7. When linking to your app from Messenger, you can present people with paid content so long as free shareable content is clearly available on the landing page.
    8. Implement App Events in your app, including activateApp and purchase events if your app offers in-app purchases.
    9. Optimized and featured functionality, including the availability of calls-to-action on content and in-Messenger discovery, is made available within our sole discretion and can be removed at any time.

16. Definitions

1. “App” means any technical integration we have assigned an app identification number.
2. "Account Information" consists of: name, email, gender, birthday, current city and profile picture URL.
3. “User data” means any data, including a person's content or information that you or third parties obtain from or through Facebook.
4. "SDK" means any object code library, sample source code, or documentation you receive from us that helps you create apps for use with the Facebook Platform.
5. By "Facebook" or "Facebook Services" we mean the features and services we make available, including through (a) our website at www.facebook.com and any other Facebook branded or co-branded websites (including sub-domains, international

versions, widgets, and mobile versions); (b) our Platform; (c) social plugins such as the Like button, the Share button and other similar offerings; and (d) other media, brands, products, services, software (such as a too bar), devices, or networks now existing or later developed. Facebook reserves the right to designate, in its sole discretion, that certain of our brands, products, or services are governed by separate terms and not our SRR.

Additional Languages

العربية	中文 (香港)	中文 (台灣)	Deutsch	Español	Français	עברית
Italiano	日本語	한국어	Polski	Português (Brasil)	Türkçe	Tiếng Việt

Developers

Products	SDKs	Tools	Support	News
Facebook Login	iOS SDK	Graph API Explorer	Platform Status	Blog
Sharing	Android SDK	Open Graph Debugger	Developers Group	Developer Roadmap
Parse	JavaScript SDK	Object Browser	Preferred Developers	Showcase
Games	PHP SDK	JavaScript Test Console	Bugs	
Ads for Apps	Unity SDK	Facebook Insights		

Platform Policy

1. Build a quality product
2. Give people control
3. Protect data
4. Encourage proper use
5. Follow the law
6. Things you should know

If you use these features, follow these additional policies:

7. Login
8. Ads
9. Games
10. Payments
11. App Center
12. Open Graph
13. Social Plugins
14. Ads API
15. Definitions

Last updated November 5, 2014

Facebook Platform Policy

Other Languages

1. Build a quality product

1. Build an app that is stable and easily navigable.
2. Ensure that your app's content (including ads and user-generated content) meets our Community Standards.
3. Follow our Advertising Guidelines for your app name, icons, and description.
4. Keep your app's description and categorization up-to-date.
5. Don't confuse, deceive, defraud, mislead, spam or surprise anyone.
6. Keep your app's negative feedback below our thresholds.
7. Follow any instructions we include in our technical documentation.

2. Give people control

1. Obtain consent from people before publishing content on their behalf.
2. Use publishing permissions to help people share on Facebook, not to send people messages from your app.
3. Don't prefill captions, comments, messages, or the user message parameter of posts with content a person didn't create, even if the person can edit or remove the content before sharing.
4. Provide a publicly available and easily accessible privacy policy that explains what data you are collecting and how you will use that data.
5. You may use Account Information in accordance with your privacy policy and oth Facebook policies. All other data may only be used outside your app after you have obtained explicit user consent.
6. Include your privacy policy URL in the App Dashboard.
7. Link to your privacy policy in any app marketplace that allows you to.

8. Comply with your privacy policy.
9. Delete all of a person's data you have received from us (including friend data) if that person asks you to, unless you are required to keep it by law, regulation, or separate agreement with us. You may keep aggregated data only if no information identifying a specific person could be inferred or created from it.
10. Obtain consent from people before using their data in any ad.
11. Obtain consent from people before you give us information that you independently collected from them.
12. If you are tracking a person's activity, provide an opt-out from that tracking.
13. Provide meaningful customer support for your app, and make it easy for people to contact you.
14. If people come to your app from the Facebook app on iOS, give them an option to go back to the Facebook app by using the Back to Facebook banner provided in our SDK.
15. If people come to your app from the Facebook app on Android, don't prevent them from going back to Facebook when they press the system back button.

3. Protect data

1. Protect the information you receive from us against unauthorized access or use.
2. Only show data obtained from a user access token on the devices associated with that token.
3. Only use friend data (including friends list) in the person's experience in your app.
4. If you cache data you receive from us, use it to improve your app's user experience and keep it up to date.
5. Don't proxy, request or collect Facebook usernames or passwords.
6. Keep private your secret key and access tokens. You can share them with an agent acting to operate your app if they sign a confidentiality agreement.
7. If you use any partner services, make them sign a contract to protect any information you obtained from us, limit their use of that information, and keep it confidential.
8. Keep Facebook user IDs within your control. Contract with any providers who help you build or run your app to ensure that they keep the user IDs secure and confidential and comply with our policies. If you need an anonymous unique identifier to share with third parties, use our mechanism.
9. Don't sell, license, or purchase any data obtained from us or our services.
10. Don't transfer any data that you receive from us (including anonymous, aggregate, or derived data) to any ad network, data broker or other advertising or monetization-

related service.

11. Don't put Facebook data in a search engine or directory, or include web search functionality on Facebook.

12. If you are acquired by or merge with a third party, you can continue to use our data only within your app.

13. If you stop using Platform, promptly delete all user data you have received from us (absent explicit consent from people). You can keep Account Information if you have presented your privacy policy within your app.

14. If you use friend data from Facebook to establish social connections in your app, only do so if each person in that connection has granted you access to that information.

4. Encourage proper use

1. Add something unique to the community. Don't replicate core functionality that Facebook already provides.

2. Respect the way Facebook looks and functions. Don't offer experiences that change it.

3. If you're building an app with a personalized or social experience, enable people to easily share on Facebook content they've created.

4. Respect the limits we've placed on Facebook functionality.

5. Only incentivize a person to log into your app, enter a promotion on your app's Page, or check-in at a place. Don't incentivize other actions.

6. Encourage people to accurately tag and share content.

7. If your service integrates a person's data into a physical product, only create a physical product for that person's personal and non-commercial use.

8. Don't build an app whose primary purpose is to redirect people off of Facebook.

9. If you want to use our logos or brand, follow the guidelines in the Facebook Brand Resource and Permissions Center. Ad networks and data brokers must get our written permission before using our Platform, logos, or trademarks.

10. Don't sell, transfer or sublicense our code, APIs, or tools to anyone.

11. Only use our SDKs to develop and distribute apps for use with the Facebook Platform. You may also distribute any code libraries or sample source code included in the SDKs for inclusion in such apps.

12. Don't modify, translate, create derivative works of, or reverse engineer any SDK or its components.

13. Be honest about your relationship with Facebook when talking to the press or users.

Comply with our Developer PR Guidelines and get approval from us before issuing any formal press release or blog post mentioning Facebook.

14. If you use the Like button on iOS or Android, don't collect or use any information from it.

5. Follow the law

1. You are responsible for restricting access to your content in accordance with all applicable laws and regulations, including geo-filtering or age-gating access where required.

2. Don't provide or promote content that infringes upon the rights of any third party.

3. Ensure that you own or secure all rights necessary to display, distribute and deliver all content in your app.

4. Satisfy all licensing, reporting and payout obligations to third parties in connection with your app.

5. If your app contains content submitted or provided by third parties:

   a. In the United States, you must take all steps required to fall within the applicable safe harbors of the Digital Millennium Copyright Act including designating an agent to receive notices of claimed infringement, instituting a repeat infringer termination policy and implementing a notice and takedown process.

   b. In other countries, you must comply with local copyright laws and implement an appropriate notice and takedown process for when you receive a notice of claimed infringement.

6. Don't knowingly share information with us that you have collected from children under the age of 13.

7. Web sites or services directed to children under 13: If you use Social Plugins or our JavaScript SDK for Facebook on sites and services that are directed to children under 13, you are responsible for complying with all applicable laws. For example, if your web site or service is directed to children in the United States, or knowingly collects personal information from children in the United States, you must comply with the U.S. Children's Online Privacy Protection Act. You must also adhere to our usage notes.

8. Comply with all applicable laws and regulations in the jurisdiction where your app is available. Do not expose Facebook or people who use Facebook to harm or legal liability as determined by us in our sole discretion.

9. If applicable, comply with the Video Privacy Protection Act (VPPA) and obtain any opt-in consent necessary to share data on Facebook.

10. You agree to indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to any claim against us related to your service, actions, content or information.

6. Things you should know

1. We can analyze your app, content, and data for any purpose, including commercial.
2. We can monitor or collect data related to your use of SDKs.
3. We will use information we receive from you or in connection with your Platform integration in accordance with our Data Policy.
4. You give us all rights necessary to enable your app to work with Facebook, including the right to incorporate information you provide to us into other parts of Facebook, and the right to attribute the source of information using your name or logos.
5. We may share your contact info with people who want to contact you.
6. We may use your name, logos, content, and information, including screenshots and video captures of your app, to demonstrate or feature your use of Facebook, worldwide and royalty-free.
7. You give us the right to link to or frame your app, and place content, including ads, around your app. If you use our social plugins, feed dialog or share button, you also give us permission to use and allow others to use such links and content on Facebook.
8. We can audit your app to ensure it is safe and does not violate our Terms. If requested, you must provide us with proof that your app complies with our terms.
9. We can create apps or products that offer features and services similar to your app.
10. We don't guarantee that Platform will always be free.
11. If you exceed 5M MAU, 100M API calls per day, or 50M impressions per day, you may be subject to additional terms.
12. Facebook and its licensors reserve all right, title and interest, including all intellectual property and other proprietary rights, in and to all SDKs.
13. Any SDKs you receive from us are provided to you on an "as is" basis, without warranty of any kind.
14. We can issue a press release describing our relationship with you.
15. We may enforce against your app or web site if we conclude that your app violates our terms or is negatively impacting the Platform. We may or may not notify you in advance.
16. Enforcement is both automated and manual, and can include disabling your app, restricting you and your app's access to platform functionality, requiring that you delete data, terminating our agreements with you or any other action that we deem appropriate.

17. We communicate with developers through Developer Alerts and email from the fb.com or facebookmail.com domain. Ensure that the email address associated with your Facebook account and the email address registered to the app are current and that you don't filter out these messages.

18. We may change these terms at any time without prior notice. Please check them regularly. Your continued use of Platform constitutes acceptance of those changes.

19. If you use Social Plugins, Facebook SDKs, or operate a Platform app or website, you must follow our Statement of Rights and Responsibilities and these additional rules unless you have our written permission to do otherwise.

7. Login

1. Verify that you have integrated Login correctly. Your app shouldn't crash or hang during the testing process.

2. Native iOS and Android apps that implement Facebook Login must use our official SDKs for login.

3. Use a clearly branded "Login with Facebook" button and follow the Facebook Brand Guidelines.

4. Request only the data and publishing permissions your app needs.

5. If a person declines a permission, you can prompt them again after they indicate an intent to grant you the permission.

6. Provide a "Log Out" option that functions properly and is easy to find.

8. Ads

1. If you have ads in your app on Facebook, comply with our Advertising Guidelines.

2. Avoid excessive ads. Don't let ads distract from your app's functionality.

3. Don't include ads in Page Tab apps.

4. If you use a third party ad provider to include ads in your app on Facebook, only use a provider from this list.

5. Don't include third-party ads (including for other apps) in posts, notifications, or requests.

6. Don't include or pair Platform Integrations with non-Facebook ads.

7. If you run a promotion, contest, competition, or sweepstake on Facebook, comply with our Promotions Policies.

9. Games

1. Games on Facebook.com:

   a. Don't share the same app ID with a desktop web game off of Facebook.com.

   b. Don't use your Facebook.com game or email addresses you've obtained from us to promote or link to a desktop web game off of Facebook.

   c. Use Facebook Payments as your only payment method for all in-game purchases.

   d. Use Facebook Payments offers if you reward people for actions involving third parties.

2. Desktop web games off Facebook.com:

   a. Only use Facebook Login, social plugins, and publishing channels. Don't use connections such as friends lists.

   b. During authentication, only request age, email, and publishing permissions.

3. Games on mobile:

   a. Don't share the same app ID with a desktop web game off of Facebook.com.

   b. Don't use your mobile game or email addresses you've obtained from us to promote or link to a web game off of Facebook.

4. If you want to promote online gambling, online real money games of skill, or online lotteries, first get our written permission.

5. If your game includes mandatory or optional in-app charges, explain this in your app's description.

10. Payments

1. If you use Facebook Payments, comply with the Facebook Developer Payments Terms.

2. Don't use Facebook Payments to solicit, collect or transfer funds for charitable causes without our prior permission.

3. If you're using iOS to run your app, use an iOS approved payment method.

4. If you accept payments on Facebook, only do so in your app.

11. App Center

1. Apps eligible for the Facebook App Center must use Facebook Login or have a Facebook Canvas or Page Tab app.
2. App Detail and Description:
   a. Ensure the app's name and information are grammatically correct.
   b. Ensure the app's language matches the App Center locale.
   c. Don't include URLs or use the Facebook brand.
   d. Don't include keyword lists, excessive punctuation, or non-standard symbols.
3. All Images:
   a. Use high quality, relevant images that reflect the app experience.
   b. Keep any image text concise. Don't obstruct images with text.
   c. Don't include ads, URLs or gimmicks such as Play buttons.
4. Icons:
   a. Use a transparent or colored background. If your icon requires a white background, use a colored border.
   b. If your logo has a drop shadow, use a colored background.
5. Banners:
   a. Don't include rounded edges or borders.
   b. Don't include third party logos.
6. Videos:
   a. Display the app's name.
   b. Clearly represent the purpose of the app and show accurate, relevant in-app experiences.
   c. Keep your video high-quality and high-resolution.
   d. Your video and its video cover image should be clear and recognizable. Don't include ads.

12. Open Graph

1. Open Graph Custom Actions:

a. Don't recreate actions that are already supported.

b. Write the action and object in a clear and simple way.

c. Make sure the story is grammatically correct.

d. Use English for your submission.

e. Don't indicate a person's consumption, browsing, discovering, or viewing of content.

f. Don't indicate a person has installed, visited, or connected to your app.

2. Read and Watch Actions:

a. Publish actions only after a person has been on a page for more than 10 seconds.

b. Allow people to remove stories published to Facebook on the same page where the content is hosted.

13. Social Plugins

1. Don't include or pair Platform Integrations with non-Facebook advertisements.
2. Don't sell or purchase placement of social plugins or sharer.php.
3. Don't participate in any "like" or "share" exchange programs.
4. Don't obscure or cover elements of social plugins.

14. Ads API

1. Basic and Standard Ads API access may be downgraded to Development access after 30 days of non-use.
2. Don't use the Ads API if you're an ad network or data broker.
3. Don't promote content, services, or activities contrary to our competitive position, interests, or advertising philosophy.
4. Don't provide Partner Category targeting options that differ from those offered by Facebook.
5. Don't combine multiple end-advertisers or their Facebook connections (i.e. Pages) in the same ad account.
6. Free or trial versions of an ads API app:

a. Don't allow more than 50 ad creations a day per customer.

b. Require phone or email verification on new accounts.

c. Don't allow affiliate networks to use your technology.

7. Pricing transparency:

a. Only charge fees for the use of your tools and managed services with a fixed fee or variable percentage of ad spend.

b. Proactively disclose to end advertisers the amount that you spent on Facebook advertising, using Facebook metrics (e.g., CPC, CPM rate), separate from your fees.

c. Disclose the amount you charged as fees on Facebook advertising.

d. We may disclose fees or the amount you spent on Facebook advertising to your clients if they request it.

e. We may require documentation from you to ensure your compliance with these terms.

f. Don't sell ads on a fixed CPM or CPC basis when using the Facebook advertising auction.

8. Data Collection and Use:

a. If you have Standard Ads API access and our prior written permission, you can place 1x1 pixel view tags on advertisements.

b. Ensure that any data that is collected is anonymous.

c. Only use data from an end-advertiser's campaign to optimize or measure the performance of that end-advertiser's Facebook campaign.

d. Don't use data to retarget on or off of Facebook.

e. Don't mix data obtained from us with advertising campaigns on different platforms.

f. Don't use data to build or augment any user profiles.

g. Don't use piggybacking or redirects.

h. Don't let people other than those acting on an end-advertiser's behalf access Facebook ad statistics.

9. Implement all bidding types including Optimized CPM.

10. Custom Audiences:

a. If you use custom audiences, comply with the Custom Audience Terms.

b. Only use a client's data when creating custom audiences on their behalf.

c. Only use a Facebook User ID to create custom audiences when the person whose User ID is being used has logged into the client's app and has given the necessary consent.

d. Don't sell or transfer custom audiences.

11. Revoke an end-advertiser's access to your app if we request it.

15. Definitions

1. "App" means any technical integration we have assigned an app identification number.
2. "Account Information" consists of: name, email, gender, birthday, current city and profile picture URL.
3. "User data" means any data, including a person's content or information that you or third parties obtain from or through Facebook.
4. "SDK" means any object code library, sample source code, or documentation you receive from us that helps you create apps for use with the Facebook Platform.

Additional Languages

العربية | 中文(香港) | 中文(台灣) | Deutsch | Español | Français | עברית
Italiano | 日本語 | 한국어 | Polski | Português (Brasil) | Türkçe | Tiếng Việt

Platform Policy

1. Build a quality product
2. Give people control
3. Protect data
4. Encourage proper use
5. Follow the law
6. Things you should know

If you use these features, follow these additional policies:

7. Login
8. Ads
9. Games
10. Payments
11. App Center
12. Open Graph
13. Social Plugins
14. Ads API
15. Definitions

1. Build a quality product

1. Build an app that is stable and easily navigable.
2. Ensure that your app's content (including ads and user-generated content) meets our Community Standards.
3. Follow our Advertising Guidelines for your app name, icons, and description.
4. Keep your app's description and categorization up-to-date.
5. Don't confuse, deceive, defraud, mislead, spam or surprise anyone.
6. Keep your app's negative feedback below our thresholds.
7. Follow any instructions we include in our technical documentation.

2. Give people control

1. Obtain consent from people before publishing content on their behalf.
2. Use publishing permissions to help people share on Facebook, not to send people messages from your app.
3. Ensure that all content in the user message parameter is entered by the user. Don't pre-fill. This includes posts, messages, comments, and captions.
4. Provide a publicly available and easily accessible privacy policy that explains what data you are collecting and how you will use that data.
5. Include your privacy policy URL in the App Dashboard.
6. Link to your privacy policy in any app marketplace that allows you to.
7. Comply with your privacy policy.
8. Delete all of a person's data you have received from us (including friend data) if that person asks you to, unless you are required to keep it by law, regulation, or separate agreement with us. You may keep aggregated data only if no information identif a specific person could be inferred or created from it.
9. Obtain consent from people before using their data in any ad.
10. Obtain consent from people before you give us information that you independently collected from them.
11. If you are tracking a person's activity, provide an opt-out from that tracking.

12. Provide meaningful customer support for your app, and make it easy for people to contact you.

13. If people come to your app from the Facebook app on iOS, give them an option to go back to the Facebook app by using the Back to Facebook banner provided in our SDK.

14. If people come to your app from the Facebook app on Android, don't prevent them from going back to Facebook when they press the system back button.

3. Protect data

1. Protect the information you receive from us against unauthorized access or use.

2. Only show data obtained from a user access token on the devices associated with that token.

3. Only use friend data (including friends list) in the person's experience in your app.

4. If you cache data you receive from us, use it to improve your app's user experience and keep it up to date.

5. Don't proxy, request or collect Facebook usernames or passwords.

6. Keep private your secret key and access tokens. You can share them with an agent acting to operate your app if they sign a confidentiality agreement.

7. If you use any partner services, make them sign a contract to protect any information you obtained from us, limit their use of that information, and keep it confidential.

8. Keep Facebook user IDs within your control. Contract with any providers who help you build or run your app to ensure that they keep the user IDs secure and confidential and comply with our policies. If you need an anonymous unique identifier to share with third parties, use our mechanism.

9. Don't sell, license, or purchase any data obtained from us or our services.

10. Don't transfer any data that you receive from us (including anonymous, aggregate, or derived data) to any ad network, data broker or other advertising or monetization-related service.

11. Don't put Facebook data in a search engine or directory, or include web search functionality on Facebook.

12. If you are acquired by or merge with a third party, you can continue to use our data only within your app.

13. If you stop using Platform, promptly delete all user data you have received from us (absent explicit consent from people). You can keep basic account information if you have presented your privacy policy within your app.

14. If you use friend data from Facebook to establish social connections in your app, only do so if each person in that connection has granted you access to that information.

4. Encourage proper use

1. Add something unique to the community. Don't replicate core functionality that Facebook already provides.
2. Respect the way Facebook looks and functions. Don't offer experiences that change it.
3. If you're building an app with a personalized or social experience, enable people to easily share on Facebook content they've created.
4. Respect the limits we've placed on Facebook functionality.
5. Only incentivize a person to log into your app, like your app's Page, enter a promotion on your app's Page, or check-in at a place. Don't incentivize other actions. Effective November 5th, 2014, you may no longer incentivize people to like your app's Page.
6. Encourage people to accurately tag and share content.
7. If your service integrates a person's data into a physical product, only create a physical product for that person's personal and non-commercial use.
8. Don't build an app whose primary purpose is to redirect people off of Facebook.
9. If you want to use our logos or brand, follow the guidelines in the Facebook Brand Resource and Permissions Center. Ad networks and data brokers must get our written permission before using our Platform, logos, or trademarks.
10. Don't sell, transfer or sublicense our code, APIs, or tools to anyone.
11. Only use our SDKs to develop and distribute apps for use with the Facebook Platform. You may also distribute any code libraries or sample source code included in the SDKs for inclusion in such apps.
12. Don't modify, translate, create derivative works of, or reverse engineer any SDK or its components.
13. Be honest about your relationship with Facebook when talking to the press or users. Comply with our Developer PR Guidelines and get approval from us before issuing any formal press release or blog post mentioning Facebook.
14. If you use the Like button on iOS or Android, don't collect or use any information from it.

5. Follow the law

1. You are responsible for restricting access to your content in accordance with all applicable laws and regulations, including geo-filtering or age-gating access where required.

2. Don't provide or promote content that infringes upon the rights of any third party.

3. Ensure that you own or secure all rights necessary to display, distribute and deliver all content in your app.

4. Satisfy all licensing, reporting and payout obligations to third parties in connection with your app.

5. If your app contains content submitted or provided by third parties:

   a. In the United States, you must take all steps required to fall within the applicable safe harbors of the Digital Millennium Copyright Act including designating an agent to receive notices of claimed infringement, instituting a repeat infringer termination policy and implementing a notice and takedown process.

   b. In other countries, you must comply with local copyright laws and implement an appropriate notice and takedown process for when you receive a notice of claimed infringement.

6. Don't knowingly share information with us that you have collected from children under the age of 13.

7. Web sites or services directed to children under 13: If you use Social Plugins or our JavaScript SDK for Facebook on sites and services that are directed to children under 13, you are responsible for complying with all applicable laws. For example, if your web site or service is directed to children in the United States, or knowingly collects personal information from children in the United States, you must comply with the U.S. Children's Online Privacy Protection Act. You must also adhere to our usage notes.

8. Comply with all applicable laws and regulations in the jurisdiction where your app is available. Do not expose Facebook or people who use Facebook to harm or legal liability as determined by us in our sole discretion.

9. If applicable, comply with the Video Privacy Protection Act (VPPA) and obtain any opt-in consent necessary to share data on Facebook.

10. You agree to indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to any claim against us related to your service, actions, content or information.

6. Things you should know

1. We can analyze your app, content, and data for any purpose, including commercial.

2. We can monitor or collect data related to your use of SDKs.

3. We will use information we receive from you or in connection with your Platform

integration in accordance with our Data Use Policy.

4. You give us all rights necessary to enable your app to work with Facebook, including the right to incorporate information you provide to us into other parts of Facebook, and the right to attribute the source of information using your name or logos.

5. We may share your contact info with people who want to contact you.

6. We may use your name, logos, content, and information, including screenshots and video captures of your app, to demonstrate or feature your use of Facebook, worldwide and royalty-free.

7. You give us the right to link to or frame your app, and place content, including ads, around your app. If you use our social plugins, feed dialog or share button, you also give us permission to use and allow others to use such links and content on Facebook.

8. We can audit your app to ensure it is safe and does not violate our Terms. If requested, you must provide us with proof that your app complies with our terms.

9. We can create apps or products that offer features and services similar to your app.

10. We don't guarantee that Platform will always be free.

11. If you exceed 5M MAU, 100M API calls per day, or 50M impressions per day, you may be subject to additional terms.

12. Facebook and its licensors reserve all right, title and interest, including all intellectual property and other proprietary rights, in and to all SDKs.

13. Any SDKs you receive from us are provided to you on an "as is" basis, without warranty of any kind.

14. We can issue a press release describing our relationship with you.

15. We may enforce against your app or web site if we conclude that your app violates our terms or is negatively impacting the Platform. We may or may not notify you in advance.

16. Enforcement is both automated and manual, and can include disabling your app, restricting you and your app's access to platform functionality, requiring that you delete data, terminating our agreements with you or any other action that we deem appropriate.

17. We communicate with developers through Developer Alerts and email from the fb.com or facebookmail.com domain. Ensure that the email address associated with your Facebook account and the email address registered to the app are current and that you don\'t filter out these messages.

18. We may change these terms at any time without prior notice. Please check them regularly. Your continued use of Platform constitutes acceptance of those changes.

19. If you use Social Plugins, Facebook SDKs, or operate a Platform app or website, you must follow our Statement of Rights and Responsibilities and these additional rules unless you have our written permission to do otherwise.

7. Login

1. Verify that you have integrated Login correctly. Your app shouldn't crash or hang during the testing process.
2. Native iOS and Android apps that implement Facebook Login must use our official SDKs for login.
3. Use a clearly branded "Login with Facebook" button and follow the Facebook Brand Guidelines.
4. Request only the data and publishing permissions your app needs.
5. If a person declines a permission, you can prompt them again after they indicate an intent to grant you the permission.
6. Provide a "Log Out" option that functions properly and is easy to find.

8. Ads

1. If you have ads in your app on Facebook, comply with our Advertising Guidelines.
2. Avoid excessive ads. Don't let ads distract from your app's functionality.
3. Don't include ads in Page Tab apps.
4. If you use a third party ad provider to include ads in your app on Facebook, only use a provider from this list.
5. Don't include third-party ads (including for other apps) in posts, notifications, or requests.
6. Don't include or pair Platform Integrations with non-Facebook ads.
7. If you run a promotion, contest, competition, or sweepstake on Facebook, comply with our Promotions Policies.

9. Games

1. Games on Facebook.com:

   a. Don't share the same app ID with a desktop web game off of Facebook.com.

   b. Don't use your Facebook.com game or email addresses you've obtained from us to promote or link to a desktop web game off of Facebook.

c. Use Facebook Payments as your only payment method for all in-game purchases.

d. Use Facebook Payments offers if you reward people for actions involving third parties.

2. Desktop web games off Facebook.com:

   a. Only use Facebook Login, social plugins, and publishing channels. Don't use connections such as friends lists.

   b. During authentication, only request age, email, and publishing permissions.

3. Games on mobile:

   a. Don't share the same app ID with a desktop web game off of Facebook.com.

   b. Don't use your mobile game or email addresses you've obtained from us to promote or link to a web game off of Facebook.

4. If you want to promote online gambling, online real money games of skill, or online lotteries, first get our written permission.

5. If your game includes mandatory or optional in-app charges, explain this in your app's description.

10. Payments

1. If you use Facebook Payments, comply with the Facebook Developer Payments Terms.

2. Don't use Facebook Payments to solicit, collect or transfer funds for charitable causes without our prior permission.

3. If you're using iOS to run your app, use an iOS approved payment method.

4. If you accept payments on Facebook, only do so in your app.

11. App Center

1. Apps eligible for the Facebook App Center must use Facebook Login or have a Facebook Canvas or Page Tab app.

2. App Detail and Description:

   a. Ensure the app's name and information are grammatically correct.

   b. Don't include URLs or use the Facebook brand.

c. Don't include keyword lists, excessive punctuation, or non-standard symbols.

3. All Images:

   a. Use high quality, relevant images that reflect the app experience.

   b. Comply with our Facebook Brand Guidelines and Community Standards.

   c. Don't use pixelated, stretched, or distorted images.

   d. Keep any text concise. Don't obstruct the images.

   e. Don't include third-party logos, website URLs, promotional ads or 'Play' buttons.

4. Icons:

   a. Keep icons simple and free of visual clutter.

   b. Use a transparent or colored background. If your icon requires a white background, use a colored border.

   c. Icons on a white background should be in a colored frame.

   d. Icons that have rounded corners should use a colored or transparent background.

   e. If your logo has a drop shadow, place it on a colored background.

5. Cover Images:

   a. Don't significantly obscure the cover image with the icon.

6. Banners:

   a. Display the app's name.

   b. Don't include white space, rounded edges, or borders.

7. Videos:

   a. Display the app's name.

   b. Clearly represent the purpose of the app and show accurate, relevant in-app experiences.

   c. Keep your video high-quality and high-resolution. It should not be distorted or pixelated.

   d. Your video and its video cover image should be clear and recognizable. Don't include ads, excessive text, or URLs.

   e. Comply with our Facebook Brand Guidelines and Community Standards.

12. Open Graph

1. Open Graph Custom Actions:

   a. Don't recreate actions that are already supported.

   b. Write the action and object in a clear and simple way.

   c. Make sure the story is grammatically correct.

   d. Use English.

   e. Don't indicate a person's consumption, browsing, discovering, or viewing of content.

   f. Don't indicate a person has installed, visited, or connected to your app.

2. Read and Watch Actions:

   a. Publish actions only after a person has been on a page for more than 10 seconds.

   b. Allow people to remove stories published to Facebook on the same page where the content is hosted.

3. Eligibility for Additional Properties:

   a. Use action tagging only when the tagged person participated in the action.

   b. Use place tagging only when a person is at the referenced location.

   c. Use mention tagging only to mention people in the user message field.

   d. Sharing controls should be in-line whenever a person is asked to explicitly share something.

13. Social Plugins

1. Don't include or pair Platform Integrations with non-Facebook advertisements.
2. Don't sell or purchase placement of social plugins or sharer.php.
3. Don't participate in any "like" or "share" exchange programs.
4. Don't obscure or cover elements of social plugins.

14. Ads API

1. Use separate app IDs for your staging, self-service, managed service, and each client

white-labeled apps. Don't comingle these services.

2. Use our multi-client manager to structure your end advertiser accounts.

3. Don't combine multiple end-advertisers or their Facebook connections (i.e. Pages) in the same ad account.

4. Free or trial versions of an ads API app:

   a. Don't allow more than 50 ad creations a day per customer.

   b. Require phone or email verification on new accounts.

   c. Don't allow affiliate networks to use your technology.

5. Pricing transparency:

   a. Only charge fees for the use of your tools and managed services with a fixed fee or variable percentage of ad spend.

   b. Proactively disclose to end advertisers the amount that you spent on Facebook advertising, using Facebook metrics (e.g., CPC, CPM rate), separate from your fees.

   c. Disclose the amount you charged as fees on Facebook advertising.

   d. We may disclose fees or the amount you spent on Facebook advertising to your clients if they request it.

   e. We may require documentation from you to ensure your compliance with these terms.

   f. Don't sell ads on a fixed CPM or CPC basis when using the Facebook advertising auction.

6. Data Collection and Use:

   a. If you have our prior written permission, you can place 1x1 pixel view tags on advertisements.

   b. Data collected by you or the end-advertiser may only be used by you or the end-advertiser.

   c. Ensure that any data that is collected is anonymous.

   d. Only use data from an end-advertiser's campaign to optimize or measure the performance of that end-advertiser's Facebook campaign.

   e. Don't use data to retarget on or off of Facebook.

   f. Don't mix data obtained from us with advertising campaigns on different platforms.

   g. Don't use data to build or augment any user profiles.

   h. Don't use piggybacking or redirects.

   i. Don't let people other than those acting on an end-advertiser's behalf access Facebook ad statistics.

7. Separate Reporting:

   a. If you use last-click attribution, create reporting tools that separate Facebook reporting from other channels.

   b. If you support other channels, do one of the following:

   i. Create a separate Facebook tool.

   ii. Include Facebook metrics in a separate Facebook section of your tool.

   iii. Show multi-touch attribution results side-by-side with last-click attribution results.

   c. You can report Facebook mobile ads ROI metrics if they relate to other mobile ad channels.

8. Implement all bidding types including Optimized CPM.

9. Custom Audiences:

   a. If you use custom audiences, comply with the Custom Audience Terms.

   b. Only use a client's data when creating custom audiences on their behalf.

   c. Only use a Facebook User ID to create custom audiences when the person whose User ID is being used has logged into the client's app and has given the necessary consent.

   d. Don't sell or transfer custom audiences.

   e. Don't provide data or targeting options that differ from those offered by Facebook on your custom audience tool.

10. Revoke an end-advertiser's access to your app if we request it.

15. Definitions

1. "App" means any technical integration we have assigned an app identification number.

2. "Account information" consists of: name, email, gender, birthday, current city and profile picture URL.

3. "User data" means any data, including a person's content or information that you or third parties obtain from or through Facebook.

4. "SDK" means any object code library, sample source code, or documentation you receive from us that helps you create apps for use with the Facebook Platform.

Additional Languages

العربية | 中文(香港) | 中文(台灣) | Deutsch | Español | Français | עברית

Italiano | 日本語 | 한국어 | Polski | Português (Brasil) | Türkçe | Tiếng Việt

Developers

Products	SDKs	Tools	Support	News
Facebook Login	iOS SDK	Graph API Explorer	Platform Status	Blog
Sharing	Android SDK	Open Graph Debugger	Developers Group	Developer Roadmap
Parse	JavaScript SDK	Object Browser	Preferred Developers	Showcase
Games	PHP SDK	JavaScript Test Console	Bugs	
Ads for Apps	Unity SDK	Facebook Insights		

Platform Policy

1. Build a quality product
2. Give people control
3. Protect data
4. Encourage proper use
5. Follow the law
6. Things you should know

If you use these features, follow these additional policies:

7. Login
8. Ads
9. Games
10. Payments
11. App Center
12. Open Graph
13. Social Plugins
14. Ads API
15. Definitions

1. Build a quality product

1. Build an app that is stable and easily navigable.
2. Ensure that your app's content (including ads and user-generated content) meets our Community Standards.
3. Follow our Advertising Guidelines for your app name, icons, and description.
4. Keep your app's description and categorization up-to-date.
5. Don't confuse, deceive, defraud, mislead, spam or surprise anyone.
6. Keep your app's negative feedback below our thresholds.
7. Follow any instructions we include in our technical documentation.

2. Give people control

1. Obtain consent from people before publishing content on their behalf.
2. Use publishing permissions to help people share on Facebook, not to send people messages from your app.
3. Ensure that all content in the user message parameter is entered by the user. Don't pre-fill. This includes posts, messages, comments, and captions.
4. Provide a publicly available and easily accessible privacy policy that explains what data you are collecting and how you will use that data.
5. Include your privacy policy URL in the App Dashboard.
6. Link to your privacy policy in any app marketplace that allows you to.
7. Comply with your privacy policy.
8. Delete all of a person's data you have received from us (including friend data) if that person asks you to, unless you are required to keep it by law, regulation, or separate agreement with us. You may keep aggregated data only if no information identif a specific person could be inferred or created from it.
9. Obtain consent from people before using their data in any ad.
10. Obtain consent from people before you give us information that you independently collected from them.
11. If you are tracking a person's activity, provide an opt-out from that tracking.

12. Provide meaningful customer support for your app, and make it easy for people to contact you.

13. If people come to your app from the Facebook app on iOS, give them an option to go back to the Facebook app by using the Back to Facebook banner provided in our SDK.

14. If people come to your app from the Facebook app on Android, don't prevent them from going back to Facebook when they press the system back button.

3. Protect data

1. Protect the information you receive from us against unauthorized access or use.

2. Only show data obtained from a user access token on the devices associated with that token.

3. Only use friend data (including friends list) in the person's experience in your app.

4. If you cache data you receive from us, use it to improve your app's user experience and keep it up to date.

5. Don't proxy, request or collect Facebook usernames or passwords.

6. Keep private your secret key and access tokens. You can share them with an agent acting to operate your app if they sign a confidentiality agreement.

7. If you use any partner services, make them sign a contract to protect any information you obtained from us, limit their use of that information, and keep it confidential.

8. Keep Facebook user IDs within your control. Contract with any providers who help you build or run your app to ensure that they keep the user IDs secure and confidential and comply with our policies. If you need an anonymous unique identifier to share with third parties, use our mechanism.

9. Don't sell, license, or purchase any data obtained from us or our services.

10. Don't transfer any data that you receive from us (including anonymous, aggregate, or derived data) to any ad network, data broker or other advertising or monetization-related service.

11. Don't put Facebook data in a search engine or directory, or include web search functionality on Facebook.

12. If you are acquired by or merge with a third party, you can continue to use our data only within your app.

13. If you stop using Platform, promptly delete all user data you have received from us (absent explicit consent from people). You can keep basic account information if you have presented your privacy policy within your app.

14. If you use friend data from Facebook to establish social connections in your app, only do so if each person in that connection has granted you access to that information.

4. Encourage proper use

1. Add something unique to the community. Don't replicate core functionality that Facebook already provides.
2. Respect the way Facebook looks and functions. Don't offer experiences that change it.
3. If you're building an app with a personalized or social experience, enable people to easily share on Facebook content they've created.
4. Respect the limits we've placed on Facebook functionality.
5. Only incentivize a person to log into your app, like your app's Page, enter a promotion on your app's Page, or check-in at a place. Don't incentivize other actions.
6. Encourage people to accurately tag and share content.
7. If your service integrates a person's data into a physical product, only create a physical product for that person's personal and non-commercial use.
8. Don't build an app whose primary purpose is to redirect people off of Facebook.
9. If you want to use our logos or brand, follow the guidelines in the Facebook Brand Resource and Permissions Center. Ad networks and data brokers must get our written permission before using our Platform, logos, or trademarks.
10. Don't sell, transfer or sublicense our code, APIs, or tools to anyone.
11. Only use our SDKs to develop and distribute apps for use with the Facebook Platform. You may also distribute any code libraries or sample source code included in the SDKs for inclusion in such apps.
12. Don't modify, translate, create derivative works of, or reverse engineer any SDK or its components.
13. Be honest about your relationship with Facebook when talking to the press or users. Comply with our Developer PR Guidelines and get approval from us before issuing any formal press release or blog post mentioning Facebook.
14. If you use the Like button on iOS or Android, don't collect or use any information from it.

5. Follow the law

1. You are responsible for restricting access to your content in accordance with all applicable laws and regulations, including geo-filtering or age-gating access where

required.

2. Don't provide or promote content that infringes upon the rights of any third party.

3. Ensure that you own or secure all rights necessary to display, distribute and deliver all content in your app.

4. Satisfy all licensing, reporting and payout obligations to third parties in connection with your app.

5. If your app contains content submitted or provided by third parties:

   a. In the United States, you must take all steps required to fall within the applicable safe harbors of the Digital Millennium Copyright Act including designating an agent to receive notices of claimed infringement, instituting a repeat infringer termination policy and implementing a notice and takedown process.

   b. In other countries, you must comply with local copyright laws and implement an appropriate notice and takedown process for when you receive a notice of claimed infringement.

6. Don't knowingly share information with us that you have collected from children under the age of 13.

7. Web sites or services directed to children under 13: If you use Social Plugins or our JavaScript SDK for Facebook on sites and services that are directed to children under 13, you are responsible for complying with all applicable laws. For example, if your web site or service is directed to children in the United States, or knowingly collects personal information from children in the United States, you must comply with the U.S. Children's Online Privacy Protection Act. You must also adhere to our usage notes.

8. Comply with all applicable laws and regulations in the jurisdiction where your app is available. Do not expose Facebook or people who use Facebook to harm or legal liability as determined by us in our sole discretion.

9. If applicable, comply with the Video Privacy Protection Act (VPPA) and obtain any opt-in consent necessary to share data on Facebook.

10. You agree to indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to any claim against us related to your service, actions, content or information.

6. Things you should know

1. We can analyze your app, content, and data for any purpose, including commercial.

2. We can monitor or collect data related to your use of SDKs.

3. We will use information we receive from you or in connection with your Platform integration in accordance with our Data Use Policy.

4. You give us all rights necessary to enable your app to work with Facebook, including the right to incorporate information you provide to us into other parts of Facebook, and the right to attribute the source of information using your name or logos.

5. We may share your contact info with people who want to contact you.

6. We may use your name, logos, content, and information, including screenshots and video captures of your app, to demonstrate or feature your use of Facebook, worldwide and royalty-free.

7. You give us the right to link to or frame your app, and place content, including ads, around your app. If you use our social plugins, feed dialog or share button, you also give us permission to use and allow others to use such links and content on Facebook.

8. We can audit your app to ensure it is safe and does not violate our Terms. If requested, you must provide us with proof that your app complies with our terms.

9. We can create apps or products that offer features and services similar to your app.

10. We don't guarantee that Platform will always be free.

11. If you exceed 5M MAU, 100M API calls per day, or 50M impressions per day, you may be subject to additional terms.

12. Facebook and its licensors reserve all right, title and interest, including all intellectual property and other proprietary rights, in and to all SDKs.

13. Any SDKs you receive from us are provided to you on an "as is" basis, without warranty of any kind.

14. We can issue a press release describing our relationship with you.

15. We may enforce against your app or web site if we conclude that your app violates our terms or is negatively impacting the Platform. We may or may not notify you in advance.

16. Enforcement is both automated and manual, and can include disabling your app, restricting you and your app's access to platform functionality, requiring that you delete data, terminating our agreements with you or any other action that we deem appropriate.

17. We communicate with developers through Developer Alerts and email from the fb.com or facebookmail.com domain. Ensure that the email address associated with your Facebook account and the email address registered to the app are current and that you don\'t filter out these messages.

18. We may change these terms at any time without prior notice. Please check them regularly. Your continued use of Platform constitutes acceptance of those changes.

19. If you use Social Plugins, Facebook SDKs, or operate a Platform app or website, you must follow our Statement of Rights and Responsibilities and these additional rules unless you have our written permission to do otherwise.

7. Login

1. Verify that you have integrated Login correctly. Your app shouldn't crash or hang during the testing process.
2. Native iOS and Android apps that implement Facebook Login must use our official SDKs for login.
3. Use a clearly branded "Login with Facebook" button and follow the Facebook Brand Guidelines.
4. Request only the data and publishing permissions your app needs.
5. If a person declines a permission, you can prompt them again after they indicate an intent to grant you the permission.
6. Provide a "Log Out" option that functions properly and is easy to find.

8. Ads

1. If you have ads in your app on Facebook, comply with our Advertising Guidelines.
2. Avoid excessive ads. Don't let ads distract from your app's functionality.
3. Don't include ads in Page Tab apps.
4. If you use a third party ad provider to include ads in your app on Facebook, only use a provider from this list.
5. Don't include third-party ads (including for other apps) in posts, notifications, or requests.
6. Don't include or pair Platform Integrations with non-Facebook ads.
7. If you run a promotion, contest, competition, or sweepstake on Facebook, comply with our Promotions Policies.

9. Games

1. Games on Facebook.com:

   a. Don't share the same app ID with a desktop web game off of Facebook.com.

   b. Don't use your Facebook.com game or email addresses you've obtained from us to promote or link to a desktop web game off of Facebook.

   c. Use Facebook Payments as your only payment method for all in-game purchases.

d. Use Facebook Payments offers if you reward people for actions involving third parties.

2. Desktop web games off Facebook.com:

   a. Only use Facebook Login, social plugins, and publishing channels. Don't use connections such as friends lists.

   b. During authentication, only request age, email, and publishing permissions.

3. Games on mobile:

   a. Don't share the same app ID with a desktop web game off of Facebook.com.

   b. Don't use your mobile game or email addresses you've obtained from us to promote or link to a web game off of Facebook.

4. If you want to promote online gambling, online real money games of skill, or online lotteries, first get our written permission.

5. If your game includes mandatory or optional in-app charges, explain this in your app's description.

10. Payments

1. If you use Facebook Payments, comply with the Facebook Developer Payments Terms.

2. Don't use Facebook Payments to solicit, collect or transfer funds for charitable causes without our prior permission.

3. If you're using iOS to run your app, use an iOS approved payment method.

4. If you accept payments on Facebook, only do so in your app.

11. App Center

1. Apps eligible for the Facebook App Center must use Facebook Login or have a Facebook Canvas or Page Tab app.

2. App Detail and Description:

   a. Ensure the app's name and information are grammatically correct.

   b. Don't include URLs or use the Facebook brand.

   c. Don't include keyword lists, excessive punctuation, or non-standard symbols.

3. All Images:

   a. Use high quality, relevant images that reflect the app experience.

   b. Comply with our Facebook Brand Guidelines and Community Standards.

   c. Don't use pixelated, stretched, or distorted images.

   d. Keep any text concise. Don't obstruct the images.

   e. Don't include third-party logos, website URLs, promotional ads or 'Play' buttons.

4. Icons:

   a. Keep icons simple and free of visual clutter.

   b. Use a transparent or colored background. If your icon requires a white background, use a colored border.

   c. Icons on a white background should be in a colored frame.

   d. Icons that have rounded corners should use a colored or transparent background.

   e. If your logo has a drop shadow, place it on a colored background.

5. Cover Images:

   a. Don't significantly obscure the cover image with the icon.

6. Banners:

   a. Display the app's name.

   b. Don't include white space, rounded edges, or borders.

7. Videos:

   a. Display the app's name.

   b. Clearly represent the purpose of the app and show accurate, relevant in-app experiences.

   c. Keep your video high-quality and high-resolution. It should not be distorted or pixelated.

   d. Your video and its video cover image should be clear and recognizable. Don't include ads, excessive text, or URLs.

   e. Comply with our Facebook Brand Guidelines and Community Standards.

12. Open Graph

1. Open Graph Custom Actions:

   a. Don't recreate actions that are already supported.

   b. Write the action and object in a clear and simple way.

   c. Make sure the story is grammatically correct.

   d. Use English.

   e. Don't indicate a person's consumption, browsing, discovering, or viewing of content.

   f. Don't indicate a person has installed, visited, or connected to your app.

2. Read and Watch Actions:

   a. Publish actions only after a person has been on a page for more than 10 seconds.

   b. Allow people to remove stories published to Facebook on the same page where the content is hosted.

3. Eligibility for Additional Properties:

   a. Use action tagging only when the tagged person participated in the action.

   b. Use place tagging only when a person is at the referenced location.

   c. Use mention tagging only to mention people in the user message field.

   d. Sharing controls should be in-line whenever a person is asked to explicitly share something.

13. Social Plugins

1. Don't include or pair Platform Integrations with non-Facebook advertisements.
2. Don't sell or purchase placement of social plugins or sharer.php.
3. Don't participate in any "like" or "share" exchange programs.
4. Don't obscure or cover elements of social plugins.

14. Ads API

1. Use separate app IDs for your staging, self-service, managed service, and each client white-labeled apps. Don't comingle these services.

2. Use our multi-client manager to structure your end advertiser accounts.

3. Don't combine multiple end-advertisers or their Facebook connections (i.e. Pages) in the same ad account.

4. Free or trial versions of an ads API app:

   a. Don't allow more than 50 ad creations a day per customer.

   b. Require phone or email verification on new accounts.

   c. Don't allow affiliate networks to use your technology.

5. Pricing transparency:

   a. Only charge fees for the use of your tools and managed services with a fixed fee or variable percentage of ad spend.

   b. Proactively disclose to end advertisers the amount that you spent on Facebook advertising, using Facebook metrics (e.g., CPC, CPM rate), separate from your fees.

   c. Disclose the amount you charged as fees on Facebook advertising.

   d. We may disclose fees or the amount you spent on Facebook advertising to your clients if they request it.

   e. We may require documentation from you to ensure your compliance with these terms.

   f. Don't sell ads on a fixed CPM or CPC basis when using the Facebook advertising auction.

6. Data Collection and Use:

   a. If you have our prior written permission, you can place 1x1 pixel view tags on advertisements.

   b. Data collected by you or the end-advertiser may only be used by you or the end-advertiser.

   c. Ensure that any data that is collected is anonymous.

   d. Only use data from an end-advertiser's campaign to optimize or measure the performance of that end-advertiser's Facebook campaign.

   e. Don't use data to retarget on or off of Facebook.

   f. Don't mix data obtained from us with advertising campaigns on different platforms.

   g. Don't use data to build or augment any user profiles.

   h. Don't use piggybacking or redirects.

   i. Don't let people other than those acting on an end-advertiser's behalf access Facebook ad statistics.

7. Separate Reporting:

a. If you use last-click attribution, create reporting tools that separate Facebook reporting from other channels.

b. If you support other channels, do one of the following:

i. Create a separate Facebook tool.

ii. Include Facebook metrics in a separate Facebook section of your tool.

iii. Show multi-touch attribution results side-by-side with last-click attribution results.

c. You can report Facebook mobile ads ROI metrics if they relate to other mobile ad channels.

8. Implement all bidding types including Optimized CPM.

9. Custom Audiences:

a. If you use custom audiences, comply with the Custom Audience Terms.

b. Only use a client's data when creating custom audiences on their behalf.

c. Only use a Facebook User ID to create custom audiences when the person whose User ID is being used has logged into the client's app and has given the necessary consent.

d. Don't sell or transfer custom audiences.

e. Don't provide data or targeting options that differ from those offered by Facebook on your custom audience tool.

10. Revoke an end-advertiser's access to your app if we request it.

15. Definitions

1. "App" means any technical integration we have assigned an app identification number.

2. "Account information" consists of: name, email, gender, birthday, current city and profile picture URL.

3. "User data" means any data, including a person's content or information that you or third parties obtain from or through Facebook.

4. "SDK" means any object code library, sample source code, or documentation you receive from us that helps you create apps for use with the Facebook Platform.

Additional Languages

العربية | 中文(香港) | 中文(台灣) | Deutsch | Español | Français | עברית

Italiano | 日本語 | 한국어 | Polski | Português (Brasil) | Türkçe | Tiếng Việt

Developers

Products
- Facebook Login
- Sharing
- Parse
- Games
- Ads for Apps

SDKs
- iOS SDK
- Android SDK
- JavaScript SDK
- PHP SDK
- Unity SDK

Tools
- Graph API Explorer
- Open Graph Debugger
- Object Browser
- JavaScript Test Console
- Facebook Insights

Support
- Platform Status
- Developers Group
- Preferred Developers
- Bugs

News
- Blog
- Developer Roadmap
- Showcase

Introduction

Date of Last Revision: August 20, 2013

Facebook Platform is an extension of Facebook, whose mission is to make the world more open and connected.

This agreement was written in English (US). To the extent any translated version of this agreement conflicts with the English version, the English version controls.

Additional Languages

Principles

Create a great user experience

- Build social and engaging applications
- Give users choice and control
- Help users share expressive and relevant content

Be trustworthy

- Respect privacy
- Don't mislead, confuse, defraud, or surprise users
- Don't spam - encourage authentic communications

I. Features and Functionality

1. You must not violate any law or the rights of any individual or entity, and must not expose Facebook or Facebook users to harm or legal liability as determined by us in our sole discretion. In particular you will (if applicable): comply with the Video Privacy Protection Act (VPPA), and obtain any opt-in consent necessary from users so that user data subject to the VPPA may be shared on Facebook. You represent that any disclosure to us will not be incidental to the ordinary course of your business.
2. You must not include functionality that proxies, requests or collects Facebook usernames or passwords.
3. You must not circumvent (or claim to circumvent) our intended limitations on core Facebook features and functionality.
4. If you offer a service for a user that integrates user data into a physical product (such as a scrapbook or calendar), you must only create a physical product for that user's personal and non-commercial use.
5. If you exceed, or plan to exceed, any of the following thresholds please contact us as you may be subject to additional terms: (>5M MAU) or (>100M API calls per day) or (>50M impressions per day).
6. Your app or website must offer an explicit "Log Out" option.
7. Special provision for apps on Pages: When a user visits your Page, if they have not given explicit permission by authorizing your Facebook app or directly providing information to your Page, you may only use information obtained from us and the user's interaction with your Page in connection with that Page. For example, although you may use aggregate analytics for your individual Page, you must not combine information from any other sources to customize the user's experience on your Page and may not use any information about the user's interaction with your Page in any other context (such as analytics or customization across other Pages or websites).
8. You must not use or make derivative use of Facebook icons, or use terms for Facebook features and functionality, if such use could confuse users into thinking that the reference is to Facebook features or functionality.
9. Mobile Web Apps that are running within the Facebook iOS app must not accept payments. In particular, these apps must not reference, use, or otherwise encourage the use of Facebook Payments or other non-iOS approved

payment methods.

10. Reciprocity and Replicating core functionality: (a) Reciprocity: Facebook Platform enables developers to build personalized, social experiences via the Graph API and related APIs. If you use any Facebook APIs to build personalized or social experiences, you must also enable people to easily share their experiences back with people on Facebook. (b) Replicating core functionality: You may not use Facebook Platform to promote, or to export user data to, a product or service that replicates a core Facebook product or service without our permission.
11. The primary purpose of your Canvas or Page Tab app on Facebook must not be to simply redirect users out of the Facebook experience and onto an external site.
12. You must not include data obtained from us in any search engine or directory without our written permission.
13. Special provisions for games:
    a. Desktop web games off of Facebook.com may only use Facebook Login (Authentication, excluding user connections such as friend list), Social Plugins and publishing (e.g., Feed Dialog, Stream Publish, or Open Graph). When authenticating, these games may not request additional permissions other than age, email, and our Publishing Permissions.
    b. Games on Facebook.com and mobile must not share the same app ID with desktop web games off of Facebook.com. You must not use Canvas apps to promote or link to game sites off of Facebook, and must not use emails obtained from us to promote or link to desktop web games off of Facebook.com.
    c. Games on Facebook.com or Mobile Web must use Facebook Payments as their sole and exclusive payment method for all virtual goods and currencies made available to users within the game. All other payment options are prohibited within games on Facebook.com or Mobile Web unless they go through Facebook Payments rather than directly through that payment option. By “Payment Method” we mean any method that allows a user to complete a transaction in a game that is on Facebook.com or Mobile Web, including, without limitation, by exchanging monetary value for virtual currency or virtual goods, whether directly at the time of purchase or via any previous transaction such as the user's earlier purchase of a prepaid gift card or electronic code. In-game rewards of virtual currency or virtual goods earned by users through game-play activity alone are exempt from this definition.
    d. Games on Facebook.com or Mobile Web may reward users with virtual currency or virtual goods in exchange for user actions that do not involve third parties, but rewards for user actions that involve third parties must be powered by Facebook Payments by integrating Facebook Payments offers. For example, you may not reward users with virtual currency or virtual goods in exchange for any action in which personally identifiable information is shared with a third party, you may not reward users with virtual currency or virtual goods in exchange for third party downloads, such as toolbars or ringtones, and you may not reward users with virtual currency for engaging in passive actions offered by third parties, such as watching a video, playing a mini-game, or taking an anonymous poll.

II. Data Collection and Use

1. You will only request the data you need to operate your application.
2. You may cache data you receive through use of the Facebook API in order to improve your application’s user experience, but you should try to keep the data up to date. This permission does not give you any rights to such data.
3. You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data. In addition, you will include your privacy policy URL in the App Dashboard, and must also include a link to your app's privacy policy in any app marketplace that provides you with the functionality to do so.
4. Until you display a conspicuous link to your privacy policy in your app, any data accessed by your app (including basic account information) may only be used in the context of the user's experience in that app. A user's friends' data can only be used in the context of the user's experience on your application.
5. Subject to certain restrictions, including on use and transfer, users give you their basic account information when they connect with your application. For all other data obtained through use of the Facebook API, you must obtain explicit consent from the user who provided the data to us before using it for any purpose other than displaying it back to the user on your application.

6. You will not directly or indirectly transfer any data you receive from us, including user data or Facebook User IDs, to (or use such data in connection with) any ad network, ad exchange, data broker, or other advertising or monetization related toolset, even if a user consents to such transfer or use. By indirectly we mean you cannot, for example, transfer data to a third party who then transfers the data to an ad network. By any data we mean all data obtained through use of the Facebook Platform (API, Social Plugins, etc.), including aggregate, anonymous or derivative data.
7. You will not use Facebook User IDs for any purpose outside your application (e.g., your infrastructure, code, or services necessary to build and run your application). Facebook User IDs may be used with external services that you use to build and run your application, such as a web infrastructure service or a distributed computing platform, but only if those services are necessary to running your application and the service has a contractual obligation with you to keep Facebook User IDs confidential.
8. If you need an anonymous unique identifier to share outside your application with third parties such as content partners, advertisers, or ad networks, you must use our mechanism. You must never share this anonymous unique identifier with a data broker, information broker, or any other service that we may define as such under our sole discretion.
9. You will not sell or purchase any data obtained from us by anyone. If you are acquired by or merge with a third party, you can continue to use user data within your application, but you cannot transfer data outside your application.
10. If you stop using Platform or we disable your application, you must delete all information about a user you have received from us unless: (a) it is basic account information; or (b) you have received explicit consent from the user to retain their data.
11. You cannot use a user's friend list outside of your application, even if a user consents to such use, but you can use connections between users who have both connected to your application.
12. You will delete all data you receive from us concerning a user if the user asks you to do so, and will provide an easily accessible mechanism for users to make such a request. We may require you to delete data you receive from the Facebook API if you violate our terms.
13. You will not include data you receive from us concerning a user in any advertising creative, without explicit consent from that user.
14. You must not give your secret key and access tokens to another party, unless that party is an agent acting on your behalf as an operator of your application. You are responsible for all activities that occur under your account identifiers.
15. Sharing information with Facebook:
    a. You must not use, display, share, or transfer a user's data in a manner inconsistent with your privacy policy, and must not give us information that you independently collect from a user or a user's content without that user's consent.
    b. You must provide an opt-out to users where required.
    c. You must not knowingly share information with us that you have collected from children under the age of 13 unless you obtain verifiable parental consent that covers Facebook's collection, use and disclosure in compliance with applicable law.
    d. Web sites or services directed to children under 13: If you use Social Plugins or our JavaScript SDK for Facebook on sites and services that are directed to children under 13, you are responsible for complying with all applicable laws. For example, if your web site or service is directed to children in the United States, or knowingly collects personal information from children in the United States, you must comply with the U.S. Children's Online Privacy Protection Act. You must also adhere to our usage notes.
    e. We can analyze your app, content, and data (including data about users' use of your app) for any purpose, including commercial (such as for targeting the delivery of ads on and off Facebook and indexing content for search) or to provide you with insights about the effectiveness of your ads or the use of your app.
    f. We can monitor your use of, or collect usage data related to, SDKs (including unique identifiers, associated IP addresses, version numbers, and which tools or services are being used and how they are being used).
    g. We will use information we receive from you in accordance with our Data Use Policy.

III. Content

A. General

1. Responsibility for content: You are responsible for all content of and within your application, including advertisements, user-generated content, and any content hosted, streamed or otherwise delivered to users by third parties. You must make it clear that this content is not provided by Facebook. You must also comply with the Facebook Community Standards.
2. Demographic restrictions: You are responsible for restricting access to your content in accordance with our content policies and all applicable laws and regulations. Although we provide controls to assist with this, please note that we make no representations regarding the sufficiency of any controls provided to you and that you are ultimately responsible for establishing legally compliant restrictions for each country where your app is visible.
3. Advertisements and cross-promotions:
   a. You must not include advertisements, cross-promote other applications, or provide web search functionality in content distributed through Facebook social channels.
   b. You can only utilize advertising or similar monetization related products or services from companies that appear on this list of Advertising Providers within Apps on Facebook.com.
4. Promotions: If you run, reference, or facilitate a promotion (contest, competition, or sweepstake) on Facebook, you must comply with Facebook's Promotions Guidelines.
5. Permission from Facebook: You must not promote, or provide content referencing, facilitating, or containing online gambling, online real money games of skill or online lotteries without our written permission.
6. Quality of content: you are responsible for providing users with a quality experience and must not confuse, defraud, mislead, spam or surprise users. For example, you must monitor your app's negative feedback in Application Insights to ensure it stays below our thresholds, avoid excessive advertisements or bugs, and ensure the description of your app is consistent with your app's content.

B. Content Rights

1. You agree that you will not promote or provide content that references, facilitates, contains or uses content that infringes upon the rights of any third party, including intellectual property rights, privacy, publicity, moral or other personal or proprietary rights, or that is deceptive or fraudulent.
2. You must ensure that you own or have secured all rights necessary to copy, display, distribute, deliver, render and publicly perform all content of or within your application to Facebook users in all countries where you make the content available.
3. You are responsible for all licensing, reporting and payout obligations to third parties required in connection with content of or within your application.
4. You must use commercially reasonable geo-filtering technology to block access to your application's content in countries where you are unauthorized to deliver such content, or where delivery of such content would otherwise infringe the rights of a third party.
5. Although we have no obligation to do so, in our sole discretion we may request, and you are required to provide us, proof that your application and any content of or within your application is properly licensed.

C. Third Party Content

If your application contains content submitted or provided by third parties, you must comply with the following rules:

1. In the United States you must take all steps required to fall within the applicable safe harbors of the Digital Millennium Copyright Act including designating an agent to receive notices of claimed infringement, instituting a repeat infringer termination policy and implementing a "notice and takedown" process. In other countries, you must comply with local copyright laws and implement an appropriate "notice and takedown" process upon receiving a notice of claimed infringement.

IV. Application Integration Points

1. You must not incentivize users to use (or gate content behind the use of) Facebook social channels, or imply that an incentive is directly tied to the use of our channels.
2. You must not pre-fill any of the fields associated with the following products, unless the user manually generated the content earlier in the workflow: Stream stories (user_message parameter for Facebook.streamPublish and FB.Connect.streamPublish, and message parameter for stream.publish), Photos (caption), Videos (description), Notes (title and content), Links (comment), and Jabber/XMPP.
3. If a user grants you a publishing permission, actions you take on the user's behalf must be expected by the user and consistent with the user's actions within your app.
4. Platform integrations, including social plugins:
   a. Your advertisements must not include or be paired with any Platform integrations, including social plugins such as the Like button, without our written permission.
   b. You must not sell or purchase placement of our Social Plugins, and must not facilitate or participate in any like exchange program.
   c. You must not incentivize users to Like any Page other than your own site or application, and any incentive you provide must be available to new and existing users who Like your Page.
   d. You must not obscure or cover elements of our social plugins, such as the Like button or Like box plugin.
   e. Ad networks, ad exchanges, and data brokers must not use Facebook's Platform, logos, and trademarks (including, but not limited to, Platform APIs, social plugins, the Share button, and the F logo).
5. Facebook messaging (i.e., email sent to an @facebook.com address) is designed for communication between users, and not a channel for applications to communicate directly with users.

V. Enforcement

We can take enforcement action against you and any or all of your applications if we determine in our sole judgment that you or your application violates Facebook Platform Terms and Policies. Enforcement action is both automated and manual, and can include disabling your application, restricting you and your application's access to Platform functionality, terminating our agreements with you, or any other action as we in our sole discretion deem appropriate.

Communication with developers takes place via an email sent from the facebook.com or facebookmail.com domain to the contact email address registered to the application. To stay in touch, please ensure that your email address is current and that you do not filter out any such messages.

VI. Changes

We can change these Platform Policies at any time without prior notice as we deem necessary. Your continued use of Platform constitutes acceptance of those changes.

VII. Branding and Promotion Policy

1. You must follow the guidelines set forth in the Facebook Brand Resource and Permissions Center.
2. Your app's description, display name and icons must adhere to our Advertising Guidelines.

VIII. Advertising Guidelines

IX. Facebook Developer Payments Terms

Developers participating in the program for accepting payments are subject to these terms.

X. Ads API

1. Separate apps: You must use separate apps for your staging, self-service, managed service, and white-labeled apps. If you offer a white-label version of your app, you must only do so by creating a unique app for each end-advertiser (or requiring each end-advertiser to create their own app) and you must include a required field for the third party to agree to Facebook's Platform Policies.
2. Separate ad accounts: You must use separate ad accounts for each end-advertiser and use our multi-client manager functionality to structure your end-advertiser accounts. You must never combine multiple end-advertisers within the same ad account, and this includes their connections on Facebook (ex: pages and apps).
3. Freemium: If you offer a free or trial version of an ads API app, you must allow no more than 50 ad creations per day per customer, require phone or email verification for all new accounts, and prohibit affiliate networks from using your technology.
4. Pricing transparency:
   a. You must only charge fees for the use of your tools and managed services, and must only do so on a fixed fee (per campaign or period) or variable percentage of ad spend. You must disclose to your clients the actual amount that you spent on Facebook advertising based on the auction pricing, including the actual Facebook metrics (e.g. CPC, CPM rate) and the amount you charged as fees. We reserve the right to disclose this information to your client upon their request. We may require documentation from you to ensure your compliance with this policy.
   b. You must not sell ads on a fixed CPM or CPC basis when using the Facebook advertising auction without our prior permission.
5. Data collection and use:
   a. You may place 1x1 pixel view tags on certain advertisements with our prior authorization.
   b. All data collected or obtained by you or the end-advertiser, including but not limited to all view tag data that is not otherwise available through the Facebook service, and all data derived therefrom, may only be used by you or the end-advertiser on an anonymous basis to optimize and measure the performance of that end-advertiser's Facebook campaign. Neither you nor the end-advertiser may use data for the following purposes: retargeting whether on or off of the Facebook service; to commingle data across an advertiser's campaigns from multiple platforms; to build or augment any user profiles, or to use piggybacking or redirects with the 1x1 pixel tags, or for any other purpose not expressly authorized by us.
   c. You must not permit any person (other than an agent acting on the end-advertiser's behalf) to access the end-advertiser's Ad or Sponsored Story advertising statistics, including but not limited to, fixed CPM rates and any other raw, aggregate, or anonymous statistics derived from this data.
6. Separate Reporting: If you use last-click attribution, create reporting tools that separate Facebook reporting from other channels. For example, don't create reporting dashboards that directly compare Facebook Ads metrics to search or display marketing metrics on a last-click basis. If you support other channels, you must either create a separate Facebook tool, include Facebook metrics in a separate Facebook section of your tool, or show multi-touch attribution results side-by-side with last-click attribution results. You may report Facebook mobile ads ROI metrics as they relate to other mobile ads channels.
7. Self-service reporting for Homepage ads: You must include a self-service reporting dashboard, through which end-advertisers may access up-to-date reports (raw ad statistics) for all available data points of their Homepage Ad and Sponsored Story campaigns.
8. Bidding types: You must implement all bidding types, including Optimized CPM, and you must not default to a specific type (ex: you must not default to CPC and hide oCPM).
9. Custom Audiences:
   a. If you use custom audiences you must comply with the Custom Audience Terms.
   b. You may create a custom audience on a client's behalf but must only use the client's customer data to do so (ex: you must not collect or provide any additional data to create a custom audience).
   c. You must not use Facebook User IDs to create custom audiences unless the person associated with the User ID has logged into your client's app and your client has secured any necessary consent from that person (ex: you must not create a custom audience based on users who have engaged with a Facebook Page).
   d. You must not sell custom audiences, and must not transfer a custom audience to anyone without our permission.
   e. Your custom audience tool may provide the same functionality and targeting options that Facebook provides, but you must not provide additional data or targeting options.
10. Enforcement: You must immediately revoke an end-advertiser's access to your app upon our request.

XI. License

1. We give you a license to use the code, APIs, data, and tools you receive from us for use with the Facebook Platform. Don't sell, transfer, or sublicense our code, APIs, or tools to anyone without our prior written permission. If they need a license, they should get it from us.
2. Facebook SDKs:
   a. Facebook and its licensors reserve all right, title and interest, including all intellectual property and other proprietary rights, in and to all SDKs.
   b. Subject to your compliance with our Platform Policies, you may use SDKs (or any components thereof) solely to develop and distribute applications for use with the Facebook Platform, and you may also distribute any code libraries or sample source code included in the SDKs for inclusion in such applications. You will not modify, translate, create derivative works of, or reverse engineer any SDK (or any components thereof). Any SDKs you receive from us are provided to you on an "as is" basis, without warranty of any kind.

XII. Definitions

1. By "Application" we mean canvas page application, Platform integration, or any other technical integration we have assigned an application identification number.
2. By "Facebook social channel" we mean Application Info Section, Page Tab, Feed, Requests (including invites), inbox attachments, Chat, Cover, Bookmarks, or any other feature of a user profile or Facebook communication channel in which or through which an application can provide, display, or deliver content directed at, on behalf of, or by permission of a user.
3. By “basic account information” we mean: name, email, gender, birthday, current city, and profile picture URL.
4. By "Facebook Platform Terms and Policies" we mean the Statement of Rights and Responsibilities and the Platform Policies.
5. By "User data you receive from Facebook" we mean any data or content (including any images, text, or other information or materials) you receive from us, that was provided by users to us, or was associated by us with a particular user.
6. By "SDK" we mean any object code library, sample source code, or documentation you receive from us that helps you create applications for use with the Facebook Platform.

Examples and Explanations

We want you to be successful on Facebook Platform, and we believe that the best way to do so is to provide a great user experience. Our Platform Policies will help you do this by explaining what’s required; these examples and explanations will help you understand how to put that into practice.

Additional Languages

?????????(??)??(??)Deutsch Español Français ????? Italiano ??? ??? Polski Português (Brasil) Türkçe Ti?ng Vi?t

Text exchange between Maggie Lenz and Charity Clark

May 16, 2019, 1:50 PM

ML: Any word yet on meeting?
I am finish errands and coming back soon worried I'm missing it. Ugh I hate this time of year.

CC: Just getting off a call, then back to my parking meter. 🙄 Then, the State House! I'll text you if I hear anything when I get there.

ML: Thank you! I'll do the same if I hear anything.

CC: Rep. Kimball said tomorrow, he's not sure what time, but likely 9 am.

ML: Thank you so much!

May 20, 2019, 3:21 PM

ML: Hiya! So sorry to bug you but if you have any time today would you mind giving me a call?

July 18, 2019, 2:29 PM

ML: Hi Charity, I hope you're having a wonderful summer! I'm wondering if T.J. is going to be around toward the end of September? I'm trying to arrange meetings for Kia Floyd (Facebook) and I'm hoping we could set one up with the AG. I am happy to contact his scheduler (is it Will?) but I lost his contact info. Thank you!

July 19, 2019, 9:59 AM

CC: Hi Maggie! I hope you're having a great, summer, too. I'll text you Will's contact info so you can contact him directly. I will also mention this to T.J.

[Contact Card for Will Sudbay]

ML: Thank you so much!