epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL TRADE COMMISSION

In the Matter of PayPal, Inc.

FTC File No. 162-3102

March 29, 2018

By notice published on March 5, 2018, the Federal Trade Commission ("FTC") has proposed a consent agreement with PayPal, Inc. that would settle alleged violations of federal law.[1] The Consent Agreement[2] follows the FTC's Complaint, which alleges that PayPal, through its operation of the payment service Venmo, has violated Section 5 of the FTC Act and the Gramm-Leach-Bliley ("GLB") Act's Privacy and Safeguards Rules.

The Electronic Privacy Information Center ("EPIC"), a public interest research center in Washington, D.C., submits these comments to recommend specific changes to the proposed Consent Order to safeguard the privacy interests of Venmo users EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in protecting consumer privacy, and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to

---

[1] FTC, *PayPal, Inc.; Analysis to Aid Public Comment*, 82 Fed. Reg. 39,582 (March 5, 2018), https://www.federalregister.gov/documents/2018/03/05/2018-04331/paypal-inc-analysis-to-aid-public-comment.

[2] *In the Matter of PayPal, Inc.* (Decision and Order), FTC, File No. 162-3102 (March 5, 2018), https://www.ftc.gov/system/files/documents/cases/venmo_agreement_with_decision.pdf [hereinafter "Consent Agreement"].

safeguard the privacy rights of consumers.[3] EPIC has previously filed a complaint with the FTC alleging many of the same harms identified in the PayPal matter.[4] EPIC has also routinely filed many other complaints with the FTC regarding business practices that harm consumer privacy.[5]

EPIC's comments are divided into four sections. Section I sets out FTC's legal obligations in considering these comments before finalizing its consent order. Sections II and III summarize the FTC complaint and consent order. Section IV lays out EPIC's proposed modifications to the consent order. In short, the FTC should require PayPal to (1) change Venmo's default setting to private; (2) obtain affirmative express consent before enacting any changes to its privacy settings; (3) make its independent privacy assessments publicly available; (4) implement multi-factor authentication; and implement the Fair Information Practices.

I. The FTC has a legal obligation to consider public comments prior to finalizing any consent agreement.

The Administrative Procedure Act requires that the Commission take public comments before finalizing any consent agreement and gives the Commission authority to modify an

---

[3] Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; *See also* EPIC, *In the Matter of DoubleClick*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Feb. 10, 2000), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; EPIC, *In the Matter of Microsoft Corp.*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (July 26, 2001), http://epic.org/privacy/consumer/MS_complaint.pdf; EPIC, *In the Matter of Choicepoint*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Dec. 16, 2004), http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[4] *In the Matter of Uber Technologies, Inc.* (2015) (Complaint, Request for Investigation, Injunction, and Other Relief), Jun. 22, 2015, https://epic.org/privacy/internet/ftc/uber/Complaint.pdf.

[5] *In the Matter of Google Inc.* (Complaint, Request for Investigation, Injunction, and Other Relief), July 31, 2017, https://www.epic.org/privacy/ftc/google/EPIC-FTC-Google-Purchase-Tracking-Complaint.pdf; *In the Matter of Genesis Toys and Nuance Communications* (Complaint and Request for Investigation, Injunction, and Other Relief), Dec. 6, 2016, https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf; *In the Matter of Snapchat* (Complaint, Request for Investigation, Injunction and Other Relief) May, 16, 2013, https://epic.org/privacy/ftc/EPIC-Snapchat-Complaint.pdf; *In the Matter of Google, Inc.* (Complaint, Request for Investigation, Injunction, and Other Relief), Feb. 16, 2010, https://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf; *In the Matter of Facebook* (Complaint, Request for Investigation, Injunction, and Other Relief), Dec. 17, 2009, https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

agreement based on those comments**.** EPIC has previously submitted several comments to the Commission on preliminary consent orders, subject to public review, that implicate the privacy interests of consumers.[6] EPIC set out recommendations that would have established stronger data protection safeguards for consumers, consistent with the purpose of the settlement. However, to date the Commission has adopted these consent orders without any modification. Nevertheless, EPIC offers these recommendations on the Paypal/Venmo settlement to strengthen the proposed settlement and to protect the interests of Venmo users. EPIC reminds the Commission that its authority to solicit public comment is pursuant to agency regulations, and the Commission has clear authority to "modify" a consent order. Commission Rules of Practice, 16 C.F.R. § 2.34 states:

> **(c) Public comment.** Promptly after its acceptance of the consent agreement, the Commission will place the order contained in the consent agreement, the complaint, and the consent agreement on the public record for a period of 30 days, or such other period as the Commission may specify, for the receipt of comments or views from any interested person.
>
> **(e) Action following comment period.**
> **(2**) The Commission, following the comment period, may determine, on the basis of the comments or otherwise, that a Final Decision and Order that was issued in advance of the comment period should be modified. Absent agreement by respondents to the modifications, the Commission may initiate a proceeding to reopen and modify the decision and order in accordance with § 3.72(b) of this chapter or commence a new administrative proceeding by issuing a complaint in accordance with § 3.11 of this chapter.

A failure by the Commission to pursue modifications to proposed orders pursuant to public comment would therefore reflect a lack of diligence on the part of the Commission. Even if the Commission decides not to modify the settlement, it must provide a "reasoned response." *See Interstate Nat. Gas Ass'n of Am. v. F.E.R.C.*, *494 F.3d 1092, 1096 (D.C. Cir. 2007). See, e.g,*

[6] Comments of EPIC, *In the Matter of Snapchat, Inc.,* FTC File No. 132 3078 (Jun. 9, 2014), https://epic.org/apa/comments/FTC-Snapchat-Cmts.pdf; Comments of EPIC, *In the Matter of Myspace LLC,* FTC Docket No. 102 3058 (, Jun. 8, 2012),, https://epic.org/privacy/socialnet/EPIC-Myspace-comments-FINAL.pdf; Comments of EPIC, *In the Matter of Facebook, Inc.* FTC Docket No. 092 3184 (Dec. 27, 2011), https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf; Comments of EPIC, *In the Matter of Google,* FTC Docket No. 102 3136 (May 2, 2011), https://epic.org/privacy/ftc/googlebuzz/EPIC_Comments_to_FTC_Google_Buzz.pdf.

Response of FTC Secretary Donald S. Clark to EPIC, In the Matter of Google Inc., File No. 1023136, Docket No. C-4336 (Oct. 13, 2011).[7]

We also take this opportunity to remind the Commission that in 2011 EPIC submitted detailed comments (31 pages) on the then pending Facebook Consent order. While we supported the Commission's finding and many of the recommendations, we also said the FTC should require Facebook to:

- Restore the privacy settings that users had in 2009, before the unfair and deceptive practices addressed by the Complaint began
- Allow users to access all of the data that Facebook keeps about them
- Cease creating facial recognition profiles without users' affirmative consent
- Make Facebook's privacy audits publicly available to the greatest extent possible
- Cease secret post-log out tracking of users across websites

The FTC made no modifications to the proposed Facebook consent order in 2011. As a consequence, the privacy of Facebook users was significantly diminished.

II. The Commission has identified significant unfair and deceptive business practices and privacy violations by PayPal.

The FTC Complaint details numerous, significant unfair and deceptive trade practices by PayPal concerning the privacy of Venmo users.[8] In order to prevent the widespread publication of their personal financial transactions, a Venmo user must change two separate settings to make their transactions private, which is confusing and counterintuitive for the reasonable user. Specifically, the user must change two settings in the menu: "Default Audience Setting" and "Transaction Sharing

[7] *Available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzepic.pdf.
[8] *In the Matter of PayPal, Inc.* (Complaint), Federal Trade Commission [hereinafter "Complaint"]. The Complaint also describes problems transferring funds out of Venmo, but these comments will only discus the privacy and security allegations.

Setting."[9] A user who changes the Default Audience Setting from "public" to "friends" or "participants only" would reasonably believe the setting would apply to all of her transactions, but that is not the case. The user must also change the Transaction Sharing Setting from "Everyone" to "Only Me" otherwise some transactions will still be published publicly.[10] Exacerbating this problem is the inaccurate privacy policy.[11] Even the most adept user who is familiar with these policies and has adjusted her settings accordingly would not be able to control who could see her transactions.

The Commission also reviewed PayPal's unfair and deceptive data security practices. PayPal has represented to Venmo users that the company would provide "bank-grade security systems and data encryption to protect your financial information" and to "guard against unauthorized transactions and access to your personal or financial information."[12] This was simply not true. Venmo's data security practices did not meet basic industry standards. The company did not have a written information security program policy. They did not have a process for assessing reasonably foreseeable security risks. They also did not, or implement basic access safeguards such as including notifying a user when her account password or email had been changed.[13] As a result of these lax data security practices, unauthorized users were able to take over user accounts and withdraw funds.[14]

III. The Consent Agreement prohibits future misrepresentations, requires certain disclosures, and provides for internal assessments.

The Commission's Consent Agreement imposes certain limited requirements on PayPal:

Prohibited Misrepresentations: PayPal may not misrepresent the extent to which it "protects the privacy, confidentiality, security, or integrity of any covered information" including the extent to

[9] *Id.* at ¶ 19.
[10] *Id.* at ¶ 24-26.
[11] *Id.* at ¶ 30-31.
[12] *Id.* at ¶ 32.
[13] *Id.* at ¶ 32-33.
[14] *Id.* at ¶ 33.

which a user can control the disclosure of her information and the extent to which the company adheres to a particular level of security.[15]

Additional Privacy Disclosures: PayPal must disclose to each user "(1) how the User's transaction information will be shared with other Users; and (2) how the User can use privacy settings to limit or restrict the visibility or sharing of the User's transaction information on the Payment and Social Networking Service." This disclosure must be clear and conspicuous and separate from the privacy policy or similar document. It must disclose how the user's transaction information will be shared with other users and how the user can change the default settings to make her information private.[16]

GLB Rule Provisions: PayPal is "permanently restrained and enjoined from violating any provision of A. The Privacy of Consumer Financial Information Rule (Regulation P), 12 C.F.R. Part 1016; or B. The Standards for Safeguarding Consumer Information Rule, 16 C.F.R. Part 314."[17]

Biennial Assessment Requirements: PayPal must undergo biennial privacy assessments every two years. These assessments "must be completed by a qualified, objective, independent third-party professional" and occur every two years for the next 10 years. [18] Each assessment must detail specific privacy controls that PayPal has put in place, explain how the privacy controls are appropriate given PayPal's size, nature and scope of their activities, and sensitivity of the information being stored, explain how the privacy controls being used meet or exceed the provisions of the Consent Agreement, and certify that privacy controls are operating effectively and provide reasonable assurances that the privacy of consumer information will be protected.

---

[15] Order at 8.
[16] *Id.* at 9.
[17] *Id.* at 10.
[18] *Id.*

Additional Requirements: PayPal must also submit to the Commission "an acknowledgement of receipt of [the] Order" and deliver copies of the order to "(1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives having managerial responsibility for conduct related to the subject matter of the order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reports and Notices."[19] PayPal must provide signed and dated acknowledgement of receipts for all persons and entities who receive a copy of the Order within 60 days.

PayPal also must submit compliance reports to the FTC.[20] These reports must identify physical, postal, and e-mail addresses for PayPal and its subsidiaries, discuss how PayPal and its subsidiaries are in compliance with the Order, what changes the company has made to come into compliance with the Order, and notice for the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against PayPal.

PayPal must create records for 20 years and retain those records for 5 years unless otherwise specified.[21] These records include accounting records, personnel records, records of all consumer complaints directed at or forwarded to PayPal, records necessary to demonstrate compliance with the Order, copies of each unique Payment and Social Networking Service advertisement making a representation subject to this Order, and all materials relied upon to prepare the Assessments required by the Order.[22]

---

[19] *Id.* at 12.
[20] *Id.*
[21] *Id.* at 14.
[22] *Id.* at 14-15.

To allow for accurate monitoring and to determine compliance with the Order, PayPal also must submit additional compliance reports or other requested information within 10 days of receipt of a written request from a representative of the FTC.[23]

IV. The Consent Agreement should be modified to require that PayPal establish default privacy settings for its users make its privacy assessments publicly available, implement multi-factor authentication, and implement the Fair Information Practices.

EPIC supports the findings of the Commission and the limited recommendations. However, the proposed Consent Agreement is insufficient to protect the privacy and security of Venmo users. EPIC urges the Commission to make the following modifications.

a. Require PayPal to change Venmo's default settings to private.

The FTC should require PayPal to make future and past Venmo transactions private by default. The current default settings have caused users to disclose more information than they intended. By default, Venmo publicly discloses transaction information, including: names, dates, and messages.[24] But consumers rarely change default settings, and there is no evidence that Venmo users want their transactions to be public by default.[25] Venmo is first and foremost marketed as a payment app; users are told that they can download Venmo to easily reimburse their friends for meals and other daily tasks. Venmo product lead Melanie Aliperti said: "I think one of the things that differentiates Venmo from other social networks is that people really do view Venmo first and foremost as a payment app and the social aspect kind of comes secondary to it."[26] Given that the core

---

[23] *Id*.
[24] Complaint at ¶ 7.
[25] Lena Groeger, *Set It and Forget It: How Default Settings Rule the World***,** ProPublica (July 27, 2016), https://www.propublica.org/article/set-it-and-forget-it-how-default-settings-rule-the-world; Cass R. Sunstein, *Don't Underrate the Power of the Default Option,* Bloomberg (Dec. 28, 2017)**,** https://www.bloomberg.com/view/articles/2017-12-28/don-t-underrate-the-power-of-the-default-option.
[26] Kaitlyn Tiffany, *Why do you stalk people on Venmo?*, The Verge (Nov. 14, 2017) https://www.theverge.com/2017/11/14/16643192/venmo-stalking-whyd-you-push-that-button-podcast.

purpose of the app is to facilitate transactions, not publication of financial information, it is unreasonable for Venmo to assume that users want their payments to be made public by default.

On the contrary, there are many reasons to believe that users want their transactions to be private. Financial information has traditionally been considered among the most private and sensitive personal information;Venmo has subverted that norm by combining a payment app with social media. Venmo transactions can reveal a surprising amount of information and lead to inferences that may or may not be accurate. A series of New Yorker cartoons displays this well.[27] It discloses how couples manage finances[28] and a quick scroll through the public feed shows many payments for rent and utilities, revealing living arrangements. A website called vicemo.com scrapes Venmo data to create a feed of "publicly available Venmo transactions involving drugs, booze, and sex." Anyone can visit this site and, in real time, see people who are—actually or jokingly—paying each other for illicit substances or activities. It is one thing for users to selectively share this information, as part of a group joke or otherwise. It is a different thing entirely for Venmo to make user transactions public by default, without their affirmative consent.

Venmo users are especially vulnerable because the company markets to a wide range of consumers who may not be familiar with their platform. People who do not use other forms of social media use Venmo for its primary function as a payment tool, but and then due to the default settings end up revealing personal information unintentionally because of the app's default settings. Users who wish to can share their transactions publicly, but Venmo should be required to obtain their affirmative express consent.

---

[27] Olivia de Recat, *Common Venmo Charges, Decoded*, The New Yorker (Sept. 25, 2017), https://www.newyorker.com/humor/daily-shouts/common-venmo-charges-decoded?irgwc=1.

[28] Teddy Wayne, *Thanks to Venmo, We Now All Know How Cheap Our Friends Are*, N.Y. Times (July 21, 2017), https://www.nytimes.com/2017/07/21/style/venmo-cheap-friends-transaction-history.html.

PayPal's current expansion plans also pose greater risks to user privacy. For example, Venmo plans to work with retailers to capitalize on the "social" dimension of the app and has started to form partnerships with merchants.[29] Currently the merchant payments are not public by default as peer-to-peer payments are, but this may change as Venmo's business model shifts. PayPal CEO Bill Ready has said that as Venmo expands its relationships with retailers "you'll find social aspects will be not only present, but also be what's most attractive to our users."[30] If merchant transactions become public by default, users will become unwitting advertisers for the businesses they patronize whenever they use the app to pay. Facebook tried to do something similar in 2007 when it launched Facebook Beacon, which allowed a Facebook user's purchases to be publicized on their friends' News Feed after transacting with third-party sites. Users were unaware that such features were being tracked, and the privacy settings originally did not allow users to opt out. As a result of widespread criticism, Facebook Beacon was shut down in 2009.[31]

b. Prohibit PayPal from changing to user privacy settings without affirmative consent.

In addition to reestablishing privacy settings by default, the Commission should also prohibit any privacy changes made without meaningful user consent. In 2011, the FTC imposed a similar requirement on Facebook "to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences."[32] Yet, surprisingly, the proposed Order imposes no such requirement on PayPal. The requirement that PayPal not misrepresent its practices is meaningless if

---

[29] Joe Pinsker, *How in the World Does Venmo Make Money?*, The Atlantic (July 18, 2017), https://www.theatlantic.com/business/archive/2017/07/venmo-makes-money-banks/533946/.
[30] Emily Barry, *PayPal Talks Venmo and the Future of Payments*, Barron's Next (April 11, 2017), https://www.barrons.com/articles/paypal-talks-venmo-and-the-future-of-payments-1491943433.
[31] Erick Schonfeld, *Zuckerberg Saves Face, Apologizes for Beacon*, TechCrunch (Dec. 5, 2007), https://techcrunch.com/2007/12/05/zuckerberg-saves-face-apologies-for-beacon/.
[32] Press Release, Fed. Trade Comm'n, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, (Nov. 9, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

the company can surreptitiously change its privacy settings without obtaining consumers' affirmative express consent.

There is no reason why the proposed Order should not impose at least the same requirements as the Facebook Order. If the Commission fails to make this change, it must provide a reasoned response as to why it this Order is different. *See Interstate Nat. Gas*, 494 F.3d at 1096.

c. Require the FTC to release PayPal's independent privacy assessments publicly.

The FTC should amend also modify the proposed Consent Agreement to require that the Commission release PayPal's privacy assessments to the public. Releasing the mandated privacy assessments to the public is necessary to allow the public to determine whether they can safely and securely continue to use Venmo and other PayPal services. The biennial privacy assessments are a good step to ensure that PayPal truly does reform its privacy practices. However, to restore public trust in PayPal and its services, the FTC should require the privacy audits be made available to the public. Furthermore, this will help restore public trust in the FTC's enforcement authority. The recent Facebook/Cambridge Analytica scandal highlights a failure by the FTC to enforce its 2011 consent order.[33] If the FTC releases PayPal's privacy assessments it will signal that the FTC is not abdicating its authority to enforce its consent orders and protect the public.

d. Require PayPal to implement multi-factor authentication.

In 2018, multi-factor authentication should be a minimum standard requirement for all financial services. The National Institute of Standards and Technology (NIST) has already established multi-factor authentication as a core part of its "Digital Authentication Guideline" for federal government agencies.[34] Multi-factor authentication provides a robust method of establishing

---

[33] Marc Rotenberg, *How the FTC Could Have Prevented the Facebook Mess*, Techonomy (March 22, 2018), https://techonomy.com/2018/03/how-the-ftc-could-have-avoided-the-facebook-mess/.

[34] *See* Paul A. Grassi et al., *Digital Identity Guidelines*, NIST Special Publication 800-63-3 (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

that a user is who they claim to be, by requiring that they establish "something you know, something you have, and something you are."[35] For example, to withdraw cash from an ATM, one must use both a debit card (something you have) and a PIN (something you know). Venmo performs a similar function to an ATM and should likewise require multiple factors for a user to withdraw funds from her bank account. There are many different ways to implement multi-factor authentication, and the FTC does not need to require PayPal to implement a particular method. But the Commission should require PayPal take this basic security step to protect Venmo users.

e. Require PayPal to Implement the Fair Information Practices (FIPs).

The FTC should modify consent agreements, concerning companies that consumer privacy, to require that the company implement FIPs.[36] Under the FIPs, a company must (1) not have secret personal data record-keeping systems; (2) allow users to access the information stored about them and know how it is used; (3) not use personal data obtained for one purpose for a different purpose without consent; (4) allow users to correct errors in identifiable information kept about them; and (5) assure the reliability of the data for their intended use and take precautions to prevent misuse of personal data.[37]

In response to EPIC's comments in one case, the FTC Secretary wrote that "a settlement agreement is designed to address specific conduct alleged in a complaint, and may not impose additional obligations that are not reasonably related to such conduct or preventing its recurrence."[38] But in this case, the FIPs are reasonably related to PayPal's conduct and would prevent the

---

[35] Paul A. Grassi et al., *Digital Identity Guidelines*, NIST Special Publication 800-63-3 (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[36] *See, e.g., In the Matter of Compete, Inc.*, Docket No. FTC File No. 102 3155 (Nov. 19, 2012), https://epic.org/privacy/ftc/EPIC-FTC-Comments-Compete.pdf; *see also* In the Matter of Google, Inc., Docket No. FTC File No. 121 0120 (Feb. 22, 2013), https://epic.org/apa/comments/EPIC-FTC-Google-Antitrust-Comments.pdf.

[37] EPIC, *The Code of Fair Information Practices*, https://epic.org/privacy/consumer/code_fair_info.html.

[38] *Response of FTC Secretary Donald S. Clark to EPIC, In the Matter of Compete, Inc.,* File No. 1023155, Docket No. C-4384 (Feb. 20, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competeepicletter.pdf/

recurrence of similarly unfair and deceptive conduct. For example, Venmo users provided personal information to conduct a transaction, not to participate in a public feed. If Venmo decides at a later date to use transaction information as advertisements for retailers, the FIPs will prevent it from doing so without express affirmative consent. The FIPs are technology neutral and would ensure that the Consent Agreement remains relevant to PayPal's business practices over the course of the 20 years it will be in effect.

V. Conclusion

The FTC is under a legal obligation to consider these comments before finalizing the order with Venmo, and must also provide a reasoned response if it fails to modify the order as described above.

EPIC urges the Commission to adopt the changes to the proposed Order set out above.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Christine Bannan*
Christine Bannan
EPIC Administrative Law and Policy Fellow

/s/ *Sam Lester*
Sam Lester
EPIC Consumer Privacy Fellow

/s/ *Alan Butler*
Alan Butler
EPIC Senior Counsel