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

October 23, 2019

The Honorable Mike Crapo, Chairman
The Honorable Sherrod Brown, Ranking Member
U.S. Senate Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Crapo and Ranking Member Brown:

We write to you regarding your hearing on "Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation."[1] EPIC appreciates your attention to privacy, but believes this hearing's focus on ownership is misguided. An approach based on data ownership and portability will accelerate industry consolidation. It ducks the hard the problem of breaking up big tech, helps not all with data protection, and imagines markets that do not exist.

EPIC is a public-interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC is a leading advocate for consumer privacy and has appeared before this Committee on several occasions.[3]

Data portability will make it easier for companies such as Facebook to ingest the personal data of the of the firms it acquires. Data portability does not help consumers, but it facilitates mergers and consolidation.

Facebook's acquisition of WhatsApp is a case study of the consumer harm caused by data portability. Facebook now intends to integrate the personal data of WhatsApp users into Facebook, in violation of the representations that Facebook and WhatsApp made to the FTC in 2014.

In 2014, Facebook purchased WhatsApp, a text-messaging service that attracted users specifically because of strong commitments to privacy.[4] WhatsApp's founder stated in 2012 that,

---

[1] *Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation*, 116th Cong. (2019), S. Comm. on Banking, Housing, and Urban Affairs (Oct. 24, 2019), https://www.banking.senate.gov/hearings/data-ownership-exploring-implications-for-data-privacy-rights-and-data-valuation.

[2] EPIC, *About EPIC*, https://epic.org/epic/about.html.

[3] *See, e.g, Examining the Current Data Security and Breach Notification Regulatory Regime: Hearing Before the House Comm. on Financial Services, Subcomm. on Financial Institutions and Consumer Credit*, 115th Cong. (2018) (testimony of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/testimony/congress/EPIC-Testimony-HFS-2-14-18.pdf; *Cybersecurity and Data Protection in the Financial Sector: Hearing Before the House Comm. on Financial Services, Subcomm. Financial Institutions and Consumer Credit*, 112th Cong. (2011) (testimony of Marc Rotenberg, Exec. Dir., EPIC), https://financialservices.house.gov/uploadedfiles/091411rotenberg.pdf.

[4] EPIC, *In re: WhatsApp*, https://epic.org/privacy/internet/ftc/whatsapp/.

"[w]e have not, we do not and we will not ever sell your personal information to anyone."[5] EPIC and the Center for Digital Democracy urged the Federal Trade Commission to block the deal.[6] As we explained at the time:

> WhatsApp built a user base based on its commitment not to collect user data for advertising revenue. Acting in reliance on WhatsApp representations, internet users provided detailed personal information to the company including private text to close friends. Facebook routinely makes use of user information for advertising purposes and has made clear that it intends to incorporate the data of WhatsApp users into the user profiling business model. The proposed acquisition will therefore violate WhatsApp users' understanding of their exposure to online advertising and constitutes an unfair and deceptive trade practice, subject to investigation by the Federal Trade Commission.[7]

The FTC ultimately approved the merger after Facebook and WhatsApp promised not to make any changes to WhatsApp users' privacy settings.[8] However Facebook announced in 2016 that it would begin acquiring the personal information of WhatsApp users, including phone numbers, directly contradicting their previous promises to honor user privacy.[9] Following this, EPIC and CDD filed another complaint with the FTC in 2016, but the Commission has taken no further action.[10] Notably, the recent FTC order with Facebook does not include any restrictions related to WhatsApp.[11]

Meanwhile, European regulators have recognized the problem of Facebook integrating WhatsApp user data. In 2017, the European Commission fined Facebook €110 million for making misrepresentations during the Commission's investigation of the WhatsApp acquisition.[12] Facebook told the Commission it was unable to match WhatsApp user accounts with Facebook user accounts, when the company was aware that it had the technical capability to do so.[13] Germany's competition

---

[5] WhatsApp, *Why We Don't Sell Ads* (June 18, 2012), https://blog.whatsapp.com/245/Why-we-dont-sell-ads.
[6] EPIC and Center for Digital Democracy, Complaint, Request for Investigation, Injunction, and Other Relief In the Matter of WhatsApp, Inc., (Mar. 6, 2014), https://epic.org/privacy/ftc/whatsapp/WhatsApp-Complaint.pdf.
[7] *Id.* at 1.
[8] *See*, Letter from Jessica L. Rich, Dir., Bureau of Consumer Prot., Fed. Trade Comm'n, to Facebook and WhatsApp (Apr. 10, 2014), https://epic.org/privacy/internet/ftc/whatsapp/FTC-facebook-whatsapp-ltr.pdf (concerning the companies' pledge to honor WhatsApp's privacy promises).
[9] WhatsApp, *Looking Ahead for WhatsApp* (Aug. 25, 2016), https://blog.whatsapp.com/10000627/Looking-ahead-for-WhatsApp.
[10] EPIC and Center for Digital Democracy, Complaint, Request for Investigation, Injunction, and Other Relief In the Matter of WhatsApp, Inc. (Aug. 29, 2016), https://epic.org/privacy/ftc/whatsapp/EPIC-CDD-FTC-WhatsApp-Complaint-2016.pdf; Marc Rotenberg, *The Facebook-WhatsApp Lesson: Privacy Protection Necessary for Innovation*, Techonomy (May 4, 2018), https://techonomy.com/2018/05/facebook-whatsapp-lesson-privacy-protection-necessary-innovation.
[11] Decision and Order, *In re Facebook, Inc*., FTC File No. 1823109 (July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.
[12] European Commission, *Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover* (May 18, 2017), https://europa.eu/rapid/press-release_IP-17-1369_en.htm.
[13]

agency has imposed restrictions on Facebook's practice of combining user data from across its platforms, such as WhatsApp and Instagram, and prohibited the company from linking third-party data to specific Facebook user accounts.[14]

Facebook now intends to integrate WhatsApp, Instagram, and Facebook Messenger.[15] U.S. regulators are not responding to this threat to privacy and competition. Data portability would make this process easier for giants like Facebook, facilitating further consolidation in the technology sector.

A Better Approach to Privacy

Baseline federal legislation should be built on a familiar privacy framework, such as the original U.S. Code of Fair Information Practices and the widely followed OECD Privacy Guidelines. The rights and responsibilities set out in these frameworks are necessarily asymmetric: the individuals that give up their personal data to others get the rights; the companies that collect the information take on the responsibilities. This is the approach that the United States, the European Union, and others have always taken to establish and update privacy laws concerning the collection and use of personal data.

EPIC recently released *Grading on a Curve: Privacy Legislation in the 116th Congress.* EPIC's report set out the key elements of a privacy law. As it considers comprehensive data privacy legislation, Congress should include:

Strong definition of personal data

The scope of a privacy bill is largely determined by the definition of personally identifiable information or "personal data," in the terminology of the GDPR. A good definition recognizes that personal data includes both data that is explicitly associated with a particular individual and also data from which it is possible to infer the identity of a particular individual. A good definition of personal data will typically include a non-exclusive list of examples. Personal data also includes all information about an individual, including information that may be publicly available, such as zip code, age, gender, and race. All of these data elements are part of the profiles companies create and provide the basis for decision-making about the individual. So, bills that exclude publicly available information misunderstand the purpose of a privacy law.

Establishment of an Independent Data Protection Agency

Almost every democratic country in the world has an independent federal data protection agency, with the competence, authority, and resources to help ensure the protection of personal data. These agencies act as an ombudsman for the public. The United States has tried for many years to create agencies that mimic a privacy agency, such as the Privacy and Civil Liberties Oversight

[14] *Bundeskartellamt prohibits Facebook from combining user data from different sources* (July 2, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

[15] Mike Isaac, *Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger*, N.Y. Times (Jan. 25, 2019), https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html.

Board, or to place responsibilities at the Federal Trade Commission. Many now believe that the failure to establish a data protection agency in the United States has contributed to the growing incidents of data breach and identity theft. There is also reason to believe that the absence of a U.S. data protection agency could lead to the suspension of transborder data flows following recent decisions of the Court of Justice of the European Union.[16]

Individual rights (right to access, control, delete)

The purpose of privacy legislation is to give individuals meaningful control over their personal information held by others. This is accomplished by the creation of legal rights that individuals exercise against companies that choose to collect and use their personal data. These rights typically include the right to access and correct data, to limit its use, to ensure it is security protected, and also that it is deleted when no longer needed. "Notice and consent," although it appears in several of the proposed bills, has little to do with privacy protection. This mechanism allows companies to diminish the rights of consumers, and use personal data for purposes to benefit the company but not the individual.

Strong data controller obligations

Organizations that choose to collect and use personal data necessarily take on obligations for the collection and use of the data. These obligations help ensure fairness, accountability, and transparency in decisions about individuals. Together with the rights of individuals describes above, they are often described as "Fair Information Practices." Many of these obligations are found today in U.S. sectoral laws, national laws, and international conventions. These obligations include:

- Transparency about business practices
- Data collection limitations
- Use/Disclosure limitations
- Data minimization and deletion
- Purpose specification
- Accountability
- Data accuracy
- Confidentiality/security

Require Algorithmic Transparency

As automated decision-making has become more widespread, there is growing concern about the fairness, accountability, and transparency of algorithms. All individuals should have the right to know the basis of an automated decision that concerns them. Modern day privacy legislation typically includes provisions for the transparency of algorithms to help promote auditing and accountability. For example both the GDPR and the Council of Europe Privacy Convention—new laws that address emerging privacy challenges—have specific articles to ensure accountability for algorithmic-based decision-making.

[16] EPIC, *Max Schrems v. Data Protection Commissioner (CJEU - "Safe Harbor")*, https://epic.org/privacy/intl/schrems/.

Require Data Minimization and Privacy Innovation

Many U.S. privacy laws have provisions intended to minimize or eliminate the collection of personal data. Data minimization requirements reduce the risks to both consumers and businesses that could result from a data breach or cyber-attack.

Good privacy legislation should also promote privacy innovation, encouraging companies to adopt practices that provide useful services and minimize privacy risk. Privacy Enhancing Techniques ("PETs") seek to minimize the collection and use of personal data.

Prohibit take-it-or-leave-it or pay-for-privacy terms

Individuals should not be forced to trade basic privacy rights to obtain services. Such provisions undermine the purpose of privacy law: to ensure baseline protections for consumers.

Private Right of Action

Privacy laws in the United States typically make clear the consequences of violating a privacy law. Statutory damages, sometimes called "liquidated" or "stipulated" damages are a key element of US privacy law and should provide a direct benefit to those whose privacy rights are violated. Several of the bills pending in Congress rely on the Federal Trade Commission to enforce privacy rights, but the FTC is ineffective. The agency ignores most complaints it receives, does not impose fines on companies that violate privacy, and is unwilling to impose meaningful penalties on repeat offenders.[17]

Limit Government Access to Personal Data

Privacy legislation frequently includes specific provisions that limit government access to personal data held by companies. These provisions help ensure that the government collects only the data that is necessary and appropriate for a particular criminal investigation. Without these provisions, the government would be able to collect personal data in bulk from companies, a form of "mass surveillance" enabled by new technologies. The Supreme Court also recently said in the *Carpenter* case that personal data held by private companies, in some circumstances, is entitled to Constitutional protection.[18]

Do Not Preempt Stronger State Laws

A well-established principle in the United States is that federal privacy law should operate as a floor and not a celling. That means that Congress often passes privacy legislation that sets a minimum standard, or "baseline," for the country and allows individual states to develop new and innovative approaches to privacy protection. The consequences of federal preemption are potentially severe and could include both a reduction in privacy protection for many consumers, particularly in California, and also a prohibition on state legislatures addressing new challenges as they emerge.

---

[17] Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.*, FTC File No. 1823109 at 17 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

[18] *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

That could leave consumers and businesses exposed to increasing levels of data breach and identity theft from criminal hackers and foreign adversaries.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Committee on these issues.

Sincerely,

Marc Rotenberg
Marc Rotenberg
EPIC President

Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

Christine Bannan
Christine Bannan
EPIC Consumer Protection Counsel

Enclosures:
EPIC, *Grading on a Curve: Privacy Legislation in the 116th Congress* (2019)