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

Standards for Safeguarding Customer Information Request for Public Comment

Docket No. 2019-04981

August 1, 2019

By notice published on April 4, 2019, the Federal Trade Commission ("FTC") requests public comments on its Standards for Safeguarding Customer Information ("Safeguards Rule").[1] Pursuant to the FTC's notice, the Electronic Privacy Information Center ("EPIC") submits these comments to (1) express support for the FTC's decision to mandate baseline security requirements, (2) request that the Safeguard Rules apply to all organizations and companies that collect consumer data, and (3) urge the FTC impose data minimization requirements.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy issues.[2] EPIC has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of

[1] *Standards for Safeguarding Customer Information*, 84 Fed. Reg. 13158 (proposed Apr. 4, 2019) (to be codified at 16 C.F.R. pt. 314) [hereinafter Safeguards Proposed Rule Request for Comments], https://www.federalregister.gov/documents/2019/05/24/2019-10910/standards-for-safeguarding-customer-information.

[2] EPIC, About EPIC (2018), https://epic.org/epic/about.html.

consumers.[3] EPIC also filed an amicus brief in *FTC v. Wyndham*, defending the FTC's "critical role in safeguarding consumer privacy and promoting stronger security standards."[4]

EPIC has also advocated for enhanced protections for consumer privacy. EPIC has repeatedly testified to legislative bodies on the need for companies to better protect consumers against data breaches.[5] EPIC wrote amicus briefs to advocate for victims of data breaches in both *Attias v. Carefirst* and *Alleruzzo v. SuperValu, Inc*.[6] EPIC has submitted complaints to the FTC that have led to significant consent orders against Facebook and Google.[7] In September 2016, EPIC

---

[3] *See, e.g.*, Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm'r 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; DoubleClick, Inc., FTC File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief) , http://epic.org/privacy/choicepoint/fcraltr12.16.04.html; In the Matter of Snapchat, Inc. (2013) (Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/ftc/EPIC-Snapchat-Complaint.pdf; In the Matter of Scholarships.com, LLC (2013) (Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/student/EPIC-FTC-Compl-Scholarships.com.pdf.

[4] Brief of Amicus Curiae EPIC, et al., in Support of Respondent, *FTC v. Wyndham Hotels & Resorts, LLC*, 799 F.3d 236 (3d Cir. 2015), https://epic.org/amicus/ftc/wyndham/Wyndham-Amicus-EPIC.pdf.

[5] *See, e.g.*, Testimony and Statement of the Record of Marc Rotenberg, Executive Director, EPIC on "Examining the Current Data Security and Breach Notification Regulatory Regime," Before the H. Comm. on Fin. Servs., Feb 14, 2018), https://epic.org/testimony/congress/EPIC-Testimony-HFS-2-14-18.pdf; Testimony and Statement of the Record of Marc Rotenberg, Executive Director, EPIC on "Consumer Data Security and the Credit Bureaus," Before the S. Comm. on Banking, Housing, and Urban Affairs, Oct. 17, 2017, https://epic.org/privacy/testimony/EPIC-Testimony-SBC-10-17.pdf; Testimony and Statement for the Record of Marc Rotenberg, Executive Director, EPIC on "Cybersecurity and Data Protection in the Financial Sector," Before the S. Comm. on Banking, Housing, and Urban Affairs, June 21, 2011, https://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf; Testimony and Statement for the Record of Marc Rotenberg, Executive Director, EPIC, Hearing on the Discussion Draft of H.R. ____, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach, Before the H. Comm. on Energy and Com. Subcomm. on Com., Manufacturing, and Trade, June 15, 2011, http://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf.

[6] Brief of Amicus Curiae EPIC, in Support of Appellants, *Attias v. Carefirst*, No. 1:15-cv-882 (filed on July 1, 2018), https://epic.org/amicus/data-breach/carefirst/EPIC-Amicus-Attias-v-Carefirst-II.pdf; Brief of Amicus Curiae EPIC, in Support of Appellants, *Alleruzzo v. SuperValu, Inc.*, 870 F.3d 763 (8th Cir. 2017), https://epic.org/amicus/data-breach/supervalu/EPIC-Amicus-SuperValu.pdf.

[7] FTC, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises* (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-itdeceived-consumers-failing-keep ("Facebook's privacy practices were the subject of complaints filed with the FTC by the Electronic Privacy Information Center and a coalition of consumer groups."); FTC, *FTC*

submitted comments to the FTC's initial notice of proposed rulemaking on the Safeguards Rule informing the FTC of the harmful effects of data breaches and urging the FTC to adopt higher standards for data security.[8]

I. AMERICANS CONTINUE TO SUFFER FROM A DATA BREACH EPIDEMIC

Under the Gramm-Leach-Bliley ("GLB") Act, the FTC is responsible for establishing standards for data security that will prevent data breaches and protect consumer privacy.[9] Since EPIC submitted its initial comments on the FTC's Safeguards Rules in 2016, the number of data breaches of financial institutions has almost tripled.[10] In June 2019 alone, over 87,000 sensitive records were exposed by data breaches of banking and financial institutions.[11] A congressional report published in 2019 reveals that Equifax failed to adequately address known security vulnerabilities that resulted in its unprecedented, massive breach and exposed the names, addresses, phone numbers, social security numbers, and driver's license numbers of well over 100 million consumers.[12] And just this week, Capital One reported that a criminal hacker stole the personal information of 106 million people who had applied for credit, including credit scores, social security numbers, and bank account numbers.[13]

Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network: Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data (Mar. 30, 2011) ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched."), https://www.ftc.gov/newsevents/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

[8] EPIC, Comments in the Matter of Standards for Safeguarding Customer Information, Docket No. 2016-21231 (2016), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Rule-Comments-11-07-2016.pdf.

[9] 15 U.S.C. 6801(b).

[10] Bitglass, *Bitglass 2018 Financial Services Breach Report: Number of Breaches in 2018 Nearly Triple That of 2016* (2018), https://www.bitglass.com/press-releases/2018-financial-breaches-triple-2016.

[11] Identity Theft Resource Center, *Data Breach Reports* (June 30, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/07/2019-June-Data-Breach-Package.pdf.

[12] *See* S. Rep., How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach 6 (2019) [hereinafter S. Rep. on Equifax], https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf.

[13] EPIC, *Capital One Breach Sets Record* (July 30, 2019), https://epic.org/2019/07/capitol-one-breach-sets-record.html.

Instances of identity theft have steadily increased: customers filed 445,000 reports of identity theft with the Federal Trade Commission in 2018, a 20% increase from the 370,000 reports filed in 2017.[14] These breaches expose consumers to various harms, including identity theft, financial fraud, reputational harm, and emotional distress.[15] Victims of identity theft report concerns about sleep and concentration, and have trouble trusting family members and friends.[16] The ripple effects of identity theft are severe, and include:[17]

- Being denied credit cards and loans
- Being unable to open new accounts
- Cancelled credit cards
- Problems at work and loss of job opportunities
- Inability to rent an apartment

In recent years, new players in the financial market present additional risks to consumer privacy. Venmo recently violated the Safeguards Rule under the GLB Act by hiding inadequate data security systems from regulators and consumers, allowing hackers to access users' accounts and use their funds.[18] The FTC should continue to bring enforcement actions under the GLB Act for

[14] Fed. Trade Comm'n, *Consumer Sentinel Network Data Book 2018*, at 21 (2019), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018_0.pdf; Fed. Trade Comm'n, *Consumer Sentinel Network Data Book 2017*, at 21 (2018), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf.
[15] U.S. Gov't Accountability Office, GAO-19-230, *Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services* 4–6 (2019) [hereinafter *GAO Data Breaches*], https://www.gao.gov/assets/700/697985.pdf.
[16] Identity Theft Resource Center, *The Aftermath: The Non-Economic Impacts of Identity Theft 2018* 3, https://www.idtheftcenter.org/wp-content/uploads/2018/09/ITRC_Aftermath-2018_Web_FINAL.pdf.
[17] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017* 8, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf.
[18] Decision and Order, Paypal, Inc., FTC Docket No. C-4651 (May 23, 2018), https://www.ftc.gov/system/files/documents/cases/1623102-c4651_paypal_venmo_decision_and_order_final_5-24-18.pdf. *See also* Press Release, FTC, PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds

violations of the Safeguards Rules by nontraditional financial service companies like PayPal, Venmo, and Apple Pay.

Though financial institutions are often targeted for data breaches, inadequate data security in other industries have harmed consumers in similar ways. Over 70% of the total data breaches in 2018 affected industries other than banking and finance. In August 2018, hackers breached T-Mobile's security systems to access the account numbers, billing information, and email addresses of 2 million telephone customers.[19] The personal information—including names, phone numbers, addresses, and emails—of about 27 million customers were compromised in an attack against the mobile events app Ticketfly in June 2018.[20] Breaches of Google+ and Facebook also impacted over 50 million users last year.[21]

Hotels and airlines also experienced breaches of consumer data: in 2018, a breach of Marriott's customer database exposed the personal records of 500 million customers,[22] triggering calls for FTC action from members of Congress, privacy advocates and the public. Senator Bennie Thompson wrote, "I am disturbed by the evolving scale and scope of data breaches affecting Americans."[23] The U.K.'s Information Commissioner's Office (ICO) announced a proposal to fine Marriott for $124 million under the General Data Privacy Regulation for its failure to protect

---

and Privacy Settings; Violated Gramm-Leach-Bliley Act (Feb. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.

[19] Paige Leskin, *The 21 Scariest Data Breaches of 2018, Business Insider* (Dec. 30, 2018), https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12.

[20] Dani Deahl, *Ticketfly Hack Exposed the Personal Information of 27 Million Accounts*, The Verge (June 7, 2018), https://www.theverge.com/2018/6/7/17438516/ticketfly-hack-personal-information-26-million-customers-leaked.

[21] Identity Theft Resource Center, *ITRC 2018 End-of-Year Data Breach Report*, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[22] FTC, *The Marriot Data Breach* (Dec. 4, 2018), https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach.

[23] Letter from Bennie Thomson, U.S. Senator (D-MS), to Arne Sorenson, President and CEO of Marriott International (Dec. 3, 2018), https://homeland.house.gov/imo/media/doc/Marriott.pdf.

consumer information (GDPR).[24] In connection with the proposed action, Information Commissioner Elizabeth Denham stated, "Personal data has a real value so organizations have a legal duty to ensure its security, just like they would do with any other asset."[25]

Given the frequency and severity of data breaches, stronger and broadly enforceable Safeguard Rules are badly needed. The burden of preventing harm from data breaches should not fall on consumers. Following the investigation of the Equifax data breach, the U.S. Senate emphasized that "[c]onsumers . . . understand the need to protect information like online passwords, pin numbers, and Social Security numbers. But a consumer taking appropriate care of this information may not be enough to keep PII out of the hands of criminal hackers."[26] The FTC should implement its proposed plan to impose higher standards for consumer privacy, but should also encompass all industries that collect personal data and establish limits on data collection.

II. THE FTC MUST IMPLEMENT AND ENFORCE COMPREHENSIVE DATA SECURITY STANDARDS

In short, companies routinely fail to protect consumer data. Data breaches remain prevalent, often resulting in identity theft, financial fraud, and distress. As a result, consumers distrust companies' ability to safeguard their information. Though companies have greater resources and access to more information, consumers currently bear the burden of protecting their privacy.

The FTC's proposed amendments to the Safeguards Rules implement many suggestions EPIC made in comments in response to the FTC's initial notice.[27] The FTC's proposed rule imposes security standards that will help to prevent future instances of identity theft and privacy invasions.

---

[24] Press Statement, Information Commissioner's Office, *Intention to Fine Marriott International, Inc. More Than £99 Million Under GDPR for Data Breach* (July 9, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.
[25] *Id.*
[26] S. Rep. on Equifax 1.
[27] EPIC Safeguarding Rule Comments.

But while the proposed rule requires baseline, technology-neutral security measures and broadens the scope of activities that will be subject to these requirements, it does not go far enough to protect consumer data.

A. The FTC's decision to implement more specific safeguards rules will more effectively mitigate data breaches.

In the proposal, the FTC highlighted that EPIC "recommended that certain practices set forth in the FTC's Safeguards Rule Guidance, such as employee background checks, authentication requirements, and encryption, should be mandatory."[28] In response to EPIC's suggestions, the FTC has proposed new baseline security requirements for consumer data held by financial institutions.

The new rules will mitigate data breaches and reduce harm to consumers, while also maintaining enough flexibility to evolve with changes in technology and banking practices. The FTC notes that while it "agrees . . . that the flexibility of the current Safeguards Rule is a strength that allows the Rule to adapt to changing technology and threats," it believes "more specific requirements will benefit financial institutions by providing them more guidance and certainty in developing their information security programs."[29] EPIC agrees. The changes to the Safeguards Rule proposed by the agency are baseline security measures that will enhance data security for all Americans. Specific baseline requirements will reduce data breaches that expose Social Security numbers, credit card information, addresses, telephone numbers and often result in identity theft. Additionally, requiring incident response teams, encryption, and employee training reduce the per capita cost of a data breach.[30]

---

[28] *Supra* note 1, Proposed Safeguards Rule Request for Comments.
[29] Standards for Safeguarding Consumer Information, 84 Fed. Reg. 13158 (proposed Apr. 4, 2019) (to be codified at 16 C.F.R. pt. 314) [hereinafter Proposed Safeguards Rule Request for Comments], https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information
[30] Ponemon Institute, *2018 Cost of a Data Breach Study: Global Overview* 22 (2018), https://www.ibm.com/downloads/cas/861MNWN2.

EPIC supports the following requirements proposed by the FTC:

- Authentication and access controls for users
- Restricting access to physical locations containing consumer information
- Encryption of consumer information
- Multifactor authentication
- Audit trails
- Procedures for secure disposal of data once it's no longer necessary for business operations or legitimate business purposes
- Procedures for change management
- Regular tests of security systems
- Training of employees on data security measures
- Implementation of incident response plans to respond to breaches affecting confidentiality of information

B. EPIC supports the FTC's proposed broader definition of "Financial Institutions," but urges the FTC to expand the scope of the Safeguards Rules to all organizations and companies that collect consumer data.

The FTC noted that EPIC "advocated that the Commission expand the scope of the Rule to include 'all organizations and companies that collect consumer data,' such as educational institutions and commercial businesses."[31] In response, the FTC broadened the scope of the Safeguards Rule to encompass "finders," highlighting EPIC's argument that a broad range of industries "frequently collect the same sensitive information as traditional financial institutions and are subject to the same security threats."[32]

[31] *Supra* note 1, Proposed Safeguards Rule Request for Comments (citing EPIC Safeguarding Rule Comments at 1).
[32] *Id*.

The FTC's addition will expand the Safeguards Rule to cover entities that "act[] as a finder in bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate."[33] Per 12 CFR 225.86(d)(1),[34] referenced in the FTC's proposed rule, "operating an Internet web site that allows multiple buyers and sellers to exchange information concerning the products and services that they are willing to purchase or sell" is an example of a "finder service."[35] As written, the proposed rule should require baseline security measures for entities such as Facebook, as Facebook's "Marketplace" feature is a platform where buyers and sellers meet, exchange information, and negotiate. The FTC should ensure that it enforces compliance with safeguard rules from all finders, not merely those that connect buyers and sellers of financial services.

The FTC should also go further to include more activities under the definition of "financial activities." Many industries' data collection practices remain unconstrained by the FTC. As Commissioner Rebecca Kelly Slaughter emphasized in her remarks at the hearing on the FTC's Approach to Consumer Privacy:

> Large categories of personal data are not covered by our rules: what we share on social media, what we share with many retailers, including our largest online retailers, and what we share with apps and devices, even when we share personal health or relationship information.[36]

Absent agency oversight and standards for data security, companies that amass personal data about millions of consumers will fail to protect that data. Consumer's personal information will remain at risk of exposure, and victims of data breaches will continue to lack redress. These data breaches

---

[33] *Supra* note 1, Proposed Safeguards Rule Request for Comments.
[34] Which the FTC notes defines "finding" as "incidental to a financial activity." *Supra* note 1, Proposed Safeguards Rule Request for Comments.
[35] *Id.* 225.86(d)(1)(ii)(C).
[36] The FTC's Approach to Consumer Privacy 134 (Apr. 10, 2019), https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_2_4-10-19.pdf.

could be eliminated with reasonable data security measures. Studies show 85% of data breaches are preventable.[37] As Professor Danielle Citron explains, companies that collect consumer data "constitute the cheapest cost avoiders vis-à-vis individuals whose information sits in a private entity's database."[38] Customers, on the other hand, are not aware of what companies do with their information once they have it.[39] Yet, they still bear the burden of ensuring many industries keep their information safe.

C. The Safeguards Rule should require companies to minimize data collection.

EPIC explained in its comments on the Safeguards Rule that the FTC should include data minimization requirements. While the FTC has adopted several new requirements that will protect consumer safety, it should go further and require that companies minimize the amount of data they collect at the outset. Personal data that is not collected cannot be at risk of a data breach. Recognizing the need to limit private data collection, the National Telecommunications and Information Administration ("NTIA") has identified "reasonable minimization" as a "critical Privacy Outcome."[40]

The European Union General Data Protection Regulation (GDPR) required companies, among other things, to minimize collection of consumer data to what is "[a]dequate, relevant, and

---

[37] Dep't of Homeland Sec. Comput. Emergency Readiness Team, TA15-119, *Alert: Top 30 Targeted High Risk Vulnerabilities* (2016), https://www.us-cert.gov/ncas/alerts/TA15-119A.
[38] Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 Southern Cal. L. Rev. 241, 284 (2007)
[39] *Id.* at 285–86; *see also Understanding Consumer Attitudes About Privacy: Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Comm. on Energy & Commerce*, 112th Cong.; 102–03 (2011) (statement of Prof. Alessandro Acquisti) ("Research has suggested that US consumers are often ill-informed about the collection and usage of their personal information, and the consequences of those usages. This puts them in a position of asymmetric information, and sometimes disadvantage, relative to the data holders that collect and use that information."), https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg74605/pdf/CHRG112hhrg74605.pdf.
[40] Nat'l Telecomms. & Info. Admin., U.S. Dep't. Commerce, *Developing the Administration's Approach to Consumer Privacy*, Request for Comments, Docket No. 180821780-8780-01 (Oct. 11, 2018), https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrationsapproach-to-consumer-privacy.

limited to what is necessary in relation to the purposes for which they are processed."[41] The GDPR has already begun to improve consumer privacy. Whereas almost 90% of companies that have not implemented GDPR requirements reported data breaches in the last year, 74% of the companies seeking to comply with the GDPR have reported similar breaches.[42] While the FTC has proposed requiring companies to delete data it no longer needs, it has not yet imposed data minimization requirements. The FTC should follow the European Union's lead and require that companies not collect more personal information than necessary.

Members of Congress and privacy experts agree. Mark R. Warner, a U.S. Senator of Virginia and cofounder of the Senate Cybersecurity Counsel, recently noted that "[i]t seems like every other day we learn about a new mega-breach affecting the personal data of millions of Americans," and in response, we should "require data minimization."[43] In response to the Commission's recent proposed settlement with Facebook, Senators Blumenthal and Hawley reiterated the need for the FTC to "restrict the collection of certain types of information."[44]

III. CONCLUSION

For the foregoing reasons, EPIC (1) supports the inclusion of baseline data security requirements, (2) urges the FTC to adopt a broad definition of "financial activities," and (3) insists that the FTC establish strong data minimization requirements for organizations that are subject to the Safeguards Rule.

---

[41] Art. 5 § 1(c).
[42] Cisco, *Data Privacy Benchmark Study* 7 (January 2019), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf.
[43] U.S. Sen. Mark R. Warner (D-VA), Press Release, Sen. Warner on Marriott Data Breach (Nov. 30, 2018), https://www.warner.senate.gov/public/index.cfm/2018/11/sen-warner-on-marriott-data-breach.
[44] Letter from Sen. Richard Blumenthal (D-CT) and Sen. Josh Hawley (R-MO) (May 6, 2019), https://www.blumenthal.senate.gov/imo/media/doc/5.6.19_Letter%20to%20FTC%20re%20Facebook.pdf.

Given the severity of the current data breach epidemic plaguing consumers, the FTC should ensure that the Safeguards Rule encompasses all organizations that collect consumer data and that data minimization is mandated.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Christine Bannan*
Christine Bannan
EPIC Consumer Protection Counsel

/s/ *Lauren O'Brien*
Lauren O'Brien
EPIC Law Clerk