CENTER FOR DEMOCRACY & TECHNOLOGY

21 December 2018

Joseph J. Simons
Chairman

Christine S. Wilson
Commissioner

Noah Joshua Phillips
Commissioner

Rohit Chopra
Commissioner

Rebecca Kelly Slaughter
Commissioner

RE: FTC-2018-0098 -- Hearings on Competition and Consumer Protection in 21st Century: Consumer Privacy, February 12-13, 2019

The Center for Democracy and Technology (CDT) is a non-profit advocacy organization working to promote democratic values online and in new, existing, and emerging technologies. CDT pursues this mission by supporting laws, policies, and technical tools which empower users, protect privacy, and preserve individual rights online. CDT respectfully submits these comments in response to the request for public comment from the Federal Trade Commission on how to advance consumer privacy.

CDT advocates for a strong federal baseline privacy law; in the absence of this, we have argued for the Commission to more aggressively exercise its unfairness authority under Section 5 of the FTC Act to address the inadequacies of user controls and privacy self-management and information asymmetries that limit an individual's ability to make informed decisions about privacy.[1] Instead, since taking on the mantle of privacy enforcer twenty years ago, the FTC has largely relied on its deception authority under Section 5 to police data privacy matters.[2] Privacy enforcement as "enforcing privacy promises" has not provided sufficient privacy protections for individuals.

Our comments largely detail CDT's thinking of what a federal privacy framework should look like in response to the FTC's query on legal framework. However, we also respond to several of the general questions posed by the Commission.

---

[1] Comments of the Center for Democracy & Technology re: FTC Informational Injury Workshop (Oct. 27, 2017), https://cdt.org/files/2017/10/2017-1027-CDT-FTC-Informational-Injury-Comments.pdf [hereinafter CDT Info Injury Comments]; *see also* Comments of the Center for Democracy & Technology re: FTC Hearings on Competition and Consumer Protection in the 21st Century, Question 5, at 4-6 (Aug. 20, 2018), https://cdt.org/files/2018/08/CDT-FTC-comments-5-8-20-18.pdf [hereinafter CDT Remediation Comments].

[2] FED. TRADE COMM'N, PRIVACY ONLINE: REPORT TO CONGRESS 41 (1998); *see also* G.S. Hans, *Laptop Spying Case Indicates More Aggressive FTC Stance on Privacy*, CTR. FOR DEMOCRACY & TECH. (2012), https://cdt.org/blog/laptop-spying-case-indicates-more-aggressive-ftc-stance-on-privacy/.

I. General Questions

1. Sensitivity of Data & Variations in Consumer Preferences Should Not Be Used as Rationales to Further Encourage Privacy Self-Management

The Commission has asked whether privacy protections should depend upon both the sensitivity of data and consumer variation in privacy preferences. While both topics have merit and are worth discussion, it is crucial that the FTC proceed with the understanding that overemphasizing these two factors for privacy protection has created the inadequate regulatory regime under which we currently operate. The meaningful way forward is answering the difficult question of what fundamental rights and expectations individuals should have that cannot be signed away.

In the FTC's Final 2012 Privacy Report, the Commission noted that "information regarding children, financial and health information, Social Security numbers and precise geolocation data" was sensitive and, importantly, "before collecting such data, companies should first obtain affirmative express consent from consumers."[3] Six years later, it is worth asking not just what other categories of information or inferential data are sensitive but also whether relying on consent is sufficient to actually protect this information from misuse by corporate actors.

For example, recently *The New York Times* detailed how mobile apps and location analytics providers take the view that once individuals enable location services, sensitive location information is fair game.[4] This report explored how companies go through the motions of providing notice and obtaining consent while their actual practices reveal a Wild West of data sharing and use. Even the Network Advertising Initiative acknowledged the report raised "serious concerns about the adequacy of the current notice and choice protections offered for the use of location data."[5] Unfortunately, the FTC's approach continues to rely on privacy self-management to address this dynamic, when the reality is that even the most privacy-sensitive individuals cannot appropriately protect their privacy.[6]

As we highlighted to the FTC last year, when individuals wish to protect their privacy, the challenge confronting them can be extreme -- particularly with respect to the sensitive information categories identified by the FTC.[7] Individuals have limited insight into the complexity of information flows in digital

---

[3] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 59 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacyera-rapid-change-recommendations/120326privacyreport.pdf.

[4] Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[5] David LeDuc, *How the NAI Helps Protect Consumer Location Data*, NAI (Dec. 14, 2018), http://www.networkadvertising.org/blog-entry/how-nai-helps-protect-consumer-location-data/.

[6] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880, 1881 (2013) (noting that "even well-informed and rational individuals cannot appropriately self-manage their privacy").

[7] CDT Info Injury Comments, *supra* note 1, at 4-6.

systems as well as how their personal information may ultimately be used. To the extent that the Commission continues to rely on some conceivable ability of individuals to achieve their desired privacy preferences, it must acknowledge that individuals frequently lack any sort of meaningful control that is responsive to the creative ways that companies monetize user data. Recently, for instance, a team of researchers at the University of Washington explored how targeting online behavioral advertisements can be used to track the locations and activities of targeted individuals, without their knowledge or consent, as they move from home to work and beyond.[8]

In our recently released discussion draft for a federal privacy law, CDT has supported both stronger prohibitions against certain sensitive data processing for secondary purposes and placing guardrails on how data brokers share and repurpose individual's information whether or not it is sensitive. This builds on commonsense protections introduced in Vermont and echoes the Commission's own recommendations about how to address the privacy impacts of data brokers.[9]

That stated, to the extent that the Commission wishes to continue to promote privacy self-management, the FTC should provide evidence-supported guidance as to what types of disclosures and tools are useful to individuals. To its credit, the FTC has provided recommendations for online and mobile disclosures[10] and, most recently, held a workshop exploring the efficacy of disclosures in 2016.[11]

The issue is that oftentimes business incentives do not align with consumer interests when it comes to privacy notices and disclosures. In contrast to the way companies provide messaging around browser security (e.g., HTTPS indicators and "private browsing" disclosures), industry privacy disclosures are often complicated and unclear. The "AdChoices" self-regulatory icon illustrates how design can be deployed to minimize users' engagement with disclosures. The program's initial proposal for "enhanced notice" consisted of a "Power I" icon alongside descriptive phrases such as "interest based ads" and "Why did I get this ad?"[12] An industry-sponsored study from the Future of Privacy Forum tested a variety of different phrases and icons, concluding that substantial consumer education would be necessary and that the "Power I" icon actually tested worse than a competing design. Unfortunately, the final form of

[8] Paul Vines, Franziska Roesner, and Tadayoshi Kohno, Exploring ADINT: Using Ad Targeting for Surveillance on a Budget — or — How Alice Can Buy Ads to Track Bob (2017), *available at* https://adint.cs.washington.edu.
[9] *See* Joseph Jerome, *Where Are the Data Brokers?*, Slate FutureTense (Sept. 25, 2018), https://slate.com/technology/2018/09/data-brokers-senate-hearing-privacy.html.
[10] FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.
[11] FED. TRADE COMM'N, PUTTING DISCLOSURES TO THE TEST (2016), https://www.ftc.gov/system/files/documents/reports/putting-disclosures-test/disclosures-workshop-staff-summary-update.pdf.
[12] Jonathan Mayer, *Tracking the Trackers: The AdChoices Icon* (Aug. 18, 2011), http://cyberlaw.stanford.edu/blog/2011/08/tracking-trackers-adchoices-icon.

"enhanced notice"[13] included an alternative "Forward I" icon and, in some instances, the text "AdChoices."

It follows that the public needs much more insight into how companies evaluate and test the user interfaces they provide individuals to understand and manage their privacy. As we explained in comments to the FTC in August, usability and user experience should be a much larger element in conversations about legal compliance and engineering systems appropriately to account for "privacy by design."[14] It is clear that companies engage in considerable UX/UI testing of their user disclosures, settings, and controls, but what the results of those tests uncover is unknown.

Standardized disclosures and symbols, such as the recycling symbol or wheelchair icon, can be a useful form of notice, but success requires industry-wide adoption and public education.[15] Though CDT is skeptical of the ultimate efficacy of multi-layered notices, just-in-time notices, and other contextual disclosures,[16] the FTC could effectively place its thumb on the scale with respect to privacy communications. To again highlight the recent *New York Times* investigation into location data, some of the surprise of this information sharing could have been addressed through the basic adoption of mobile disclosures advanced by the National Telecommunications & Information Administration (NTIA) in 2013.[17] However, the FTC declined to endorse and companies declined to adopt this framework.[18] If the FTC does not wish to second guess how companies design and test products, CDT would encourage the Commission to more explicitly explore whether companies are engaged in design and usability decisions such as so-called "dark patterns" that may rise to the level of being either deceptive or unfair to individuals.[19]

2. The Impact of Privacy Rules on Competition and Innovation Should Not Be Overstated

[13] Future of Privacy Forum, Online Behavioral Advertising "Icon" Study (Feb. 2010), https://fpf.org/2010/02/15/online-behavioral-advertising-icon-study/; *see also* Stephanie Clifford, *A Little 'i' to Teach About Online Privacy*, N.Y. Times (Jan. 26, 2010), https://www.nytimes.com/2010/01/27/business/media/27adco.html.

[14] *See* CDT Remediation Comments, *supra* note 1.

[15] Comments of the Center for Democracy & Technology on REG 2011-02 -- Internet Communications Disclaimers (May 25, 2018), https://cdt.org/files/2018/05/CDT-FEC-Comments-REG-2011-02.pdf.

[16] See infra, pages 9-10.

[17] Joseph Hall, *NTIA Multistakeholder Process Delivers Increased App Transparency*, Ctr. for Democracy & Tech (July 25, 2013), https://cdt.org/blog/ntia-multistakeholder-process-delivers-increased-app-transparency/.

[18] For a history of the problems emerging from the NTIA multistakeholder process, see Margot E. Kaminski, *When the Default Is No Penalty: Negotiating Privacy at the NTIA*, 93 Denv. L. Rev. 925 (2016).

[19] Dark Patterns are tricks used in websites and apps that make individuals buy or sign up for services to which they did not intend. *See* Dark Patterns https://darkpatterns.org (last visited Dec. 20, 2018). See also ForbrukerRadet, Deceived By Design (June 27, 2018), *available at* https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

The current position of the Commission appears to be that privacy rules in particular skew benefits to large incumbent companies.[20] In comments to the NTIA, the FTC warned that privacy regulations could "unreasonably impede market entry or expansion by existing companies," but curiously, its support for this proposition was not that small businesses are unable to protect privacy and secure information but rather that a company's inability to use "targeted" "data-driven" advertising to reach new consumers might be an insurmountable burden.[21] This unfortunately frames both competition and innovation exclusively in the context of online behavioral advertising.

It has been argued that the GDPR has "consolidated control" of advertising technology (adtech) to Google and Facebook.[22] Both companies have significant resources to meet GDPR compliance requirements; Google made headlines by testifying before Congress that it had spent "hundreds of years of human time" to comply with the GDPR.[23] This may be accurate, but Google is also the most sophisticated company on the globe when it comes to collecting, using, and exploiting data. One would expect the privacy issues faced by the tech giant to be considerable, but these sorts of statements also raise questions as to how companies were complying with the earlier EU Data Protection Directive.[24] It also serves to highlight the tensions that seem inherent in the online advertising industry's underlying business model.

Individuals as well as regulators and lawmakers have limited insight into the complexity of information flows in digital systems and how their personal information may ultimately be used. The digital advertising ecosystem has become as complicated as an artificial neural network, and the industry amplifies this dynamic with its own marketing claims.[25] Early enforcement actions by EU data protection authorities demonstrate this problem.[26] In a recent decision against an adtech firm, the French

---

[20] Noah J. Phillips, Comm'r, Fed. Trade Comm'n, "Keep It: Maintaining Competition in the Privacy Debate," Remarks at the IGF-USA, at 8 (July 27, 2018), https://www.ftc.gov/system/files/documents/public_statements/1395934/phillips_-_internet_governance_forum_7-27-18.pdf.

[21] Comments of FTC Staff to the Nat'l Telecommunications & Info Admin., at 11 (Nov. 9, 2018), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

[22] Sam Schechner & Nick Kostov, *Google and Facebook Likely to Benefit From Europe's Privacy Crackdown*, Wall St. J. (Apr. 23, 2018), https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324.

[23] Ashley Rodriguez, *Google says it spent "hundreds of years of human time" complying with Europe's privacy rules*, Quartz (Sept. 26, 2018), https://qz.com/1403080/google-spent-hundreds-of-years-of-human-time-complying-with-gdpr/.

[24] Johnny Ryan, @johnnyryan, https://twitter.com/johnnyryan/status/1044989005413134344 (Sept. 26, 2018, 12:36 PM ET).

[25] *See, e.g.*, NAI 2017 Annual Compliance Report at 32, *available at* https://www.networkadvertising.org/sites/default/files/nai_compliance_report_2017.pdf (highlighting a compliance investigation based on public marketing materials that were "overzealous . . . in an attempt to make the technology appear more compelling to clients.").

[26] Natasha Lomas, *How a small French privacy ruling could remake adtech for good*, TechCrunch (Nov. 20, 2018), https://techcrunch.com/2018/11/20/how-a-small-french-privacy-ruling-could-remake-adtech-for-good/.

Commission nationale de l'informatique et des libertés (CNIL) criticized Vectuary for providing unclear, complicated, and not easily accessible disclosures and that user consent was not specific to processing geolocation information.[27]

While GDPR -- and the forthcoming CCPA -- may present compliance challenges for some segment of adtech companies, it is not at all clear that privacy laws are categorically harmful to innovation or competition. Recent FTC hearings have highlighted a study that concluded that European technology firms have received less venture funding since the GDPR went into effect in May,[28] which critics have seized as evidence of the GDPR's negative impact on innovation, but the study does not breakdown its results by business model.[29] Financial firms have highlighted some of the harmonization benefits of the GDPR, as well as providing "a valuable opportunity to rethink their product development process."[30] In response to suggestions GDPR would chill health research, medical researchers have argued that GDPR has "little impact on biomedical data research."[31] Technology firms can also pass the benefits of GDPR compliance to enterprise customers that use their technology.[32]

The reality is that it remains early days for the GDPR, and the full impact of the Regulation, positive or negative, is unknown.[33]

3. To Be a Successful Enforcer, the FTC Must Be Able to Shape Industry Practices

Most federal privacy proposals center the locus of enforcement activities at the Federal Trade Commission, and even absent a comprehensive federal privacy law, the FTC will continue to be active as

---

[27] For a description of the decisions, see Robin Kurzer, *Why a French ruling against a small mobile ad firm has ad tech on the defensive*, MarketingLand (Nov. 21, 2018), https://marketingland.com/why-a-french-ruling-against-a-small-mobile-ad-firm-has-ad-tech-on-the-defensive-252090.

[28] Jian Jia et al., *The Short-Run Effects of GDPR on Technology Venture Investment*, Working Paper No. 25248 (Nov. 2018), *available at* https://www.nber.org/papers/w25248.

[29] Leonid Bershidsky, *Europe's Privacy Rules Are Having Unintended Consequences*, Bloomberg (Nov. 14, 2018), https://www.bloomberg.com/opinion/articles/2018-11-14/facebook-and-google-aren-t-hurt-by-gdpr-but-smaller-firms-are.

[30] Erika Fry, *Here's What Mastercard's Chief Privacy Officer Thinks About GDPR*, Fortune (Nov. 7, 2018), http://fortune.com/2018/11/07/heres-what-mastercards-chief-privacy-officer-thinks-about-gdpr/.

[31] *See* John Mark Michael Rumbold & Barbara Pierscionek, *The Effect of the General Data Protection Regulation on Medical Research*, J. Med. Internet Res. 2017 Feb; 19(2), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5346164/.

[32] While some might argue the costs borne by technology firms are passed down to smaller firms, it may also be worth exploring whether GDPR is a case where a rising tide lifts all boats. For example, Microsoft has highlighted its efforts to help business partners "become trusted stewards of their customers' data." Julie Brill, *Microsoft's commitment to GDPR, privacy and putting customers in control of their own data*, Microsoft (May 21, 2018), https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/.

[33] Kevin Koerner, *GDPR – boosting or choking Europe's data economy?*, Deutsche Bank (June 13, 2018), https://www.dbresearch.com/servlet/reweb2.ReWEB?rwsite=RPS_EN-PROD&rwobj=ReDisplay.Start.class&document=PROD0000000000470381.

a privacy enforcement agency. However, in order to be successful, the FTC must be seen as being empowered to alter privacy-invading business practices and not simply reinforcing the status quo. CDT would encourage the Commission to provide more public guidance with respect to existing industry privacy pledges and the FTC's current consent decree model.

First, we recommend the FTC take a careful look at existing self-regulatory codes of conduct. In the absence of federal law and regulation, the Commission must largely defer to what companies voluntarily attest to. This is a model that companies have insisted works to protect privacy, even as, for example, automakers that agreed to car privacy principles have flaunted data collection practices "just because we could."[34] Last year, the Electronic Frontier Foundation (EFF) explicitly called on the FTC to investigate signatories to the Student Privacy Pledge. EFF further alleged that College Board sold student information in violation of its pledge by licensing student information when students join its Student Search Service.[35] Although this was further highlighted in another *New York Times* report this past summer,[36] College Board's status as a signatory remains under review,[37] and the FTC has not given any guidance or indication of its thinking on this behavior. While we have been critical about the overreliance on deceptive practices as the primary privacy enforcement mechanism, measuring compliance with voluntary industry standards may provide network effects that case-by-case enforcement is not inspiring now.

Second, CDT has begun to have serious concerns of the efficacy of the consent decrees with which the FTC has entered into with numerous companies.[38] The FTC has regularly held up its consent orders as an essential pillar of its privacy enforcement activities. A consent order typically imposes a 20-year period of FTC oversight and requires companies to implement privacy and security programs and perform regular independent assessments of the company's data practices. For a while, even the most ardent privacy advocates were placated as the FTC brought several major tech companies under consent orders for privacy violations.

That is no longer the case. The Facebook consent decree now serves as patient zero in underscoring the basic limitations of the FTC's existing approach. When the first headlines broke about Cambridge

[34] Jamie L. LaReau, *GM tracked radio listening habits for 3 months: Here's why*, Detroit Free Press (Oct. 1, 2018), https://www.freep.com/story/money/cars/general-motors/2018/10/01/gm-radio-listening-habits-advertising/1424294002/.
[35] Comments of the Electronic Frontier Foundation re: Student Privacy and Ed Tech (Nov. 17, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/11/00034-141966.pdf.
[36] Natasha Singer, *For Sale: Survey Data on Millions of High School Students*, N.Y. Times (July 29, 2018), https://www.nytimes.com/2018/07/29/business/for-sale-survey-data-on-millions-of-high-school-students.html.
[37] Student Privacy Pledge -- Signatories https://studentprivacypledge.org/signatories/ (last visited Dec. 18, 2018).
[38] Joseph Jerome, *Can FTC consent orders effectively police privacy?*, IAPP (Nov. 27, 2018), https://iapp.org/news/a/can-ftc-consent-orders-police-privacy/.

Analytica, the FTC issued a public statement that it was reopening an investigation into Facebook.[39] Facebook has continued to stress its commitment to its original consent order, even as the social network argues service provider provisions in the order may actually permit broad sharing of consumer data with business partners "for and at the direction of" Facebook even where those companies get broad and preferential access to information.[40] It is apparent that the Commission is under some pressure to take action against Facebook, but the FTC still faces a difficult enforcement challenge.[41] It is also unclear whether the FTC will be able to obtain a significant monetary penalty from the company under the terms of its original settlement.

Cognizant of both the FTC's limited resources and extreme resources available to the companies which the FTC is attempting to police, consent decrees do not appear to sufficiently chastising companies for their privacy malfeasance. FTC consent orders currently come with no admission of wrongdoing, and companies often provide no detail into whether or how any of their business practices will be impacted by the FTC's order. Adtech company Turn, for example, explained that it settled with the FTC to avoid "further distraction and expense so that we can continue to serve our customers" and it reiterated that the settlement "align[ed] with [its] existing practices."[42] If a consent order is only confirming a companies' existing practices, its ability to effectively address emerging privacy problems in the future is limited.

We believe a legislative solution that gives the FTC additional legal authority and personnel to more effectively police privacy is one part of the solution to this problem. Our discussion draft also includes the authority to levy fines that we think are fair but meaningful for a first-time violation of the law. However, we also believe the FTC must take on a more aggressive posture against companies that seem increasingly eager to flout their disregard for individual's privacy and autonomy.

II. Questions About Legal Frameworks

The Commission has also inquired as to the current and emerging state of data protection frameworks. The FTC must acknowledge the legal reality that the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have established a baseline against which any future proposal will be measured, and CDT would encourage the Commission to explore how best to augment these legal frameworks rather than facilitating an exercise in critiquing these laws.

---

[39] Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices (Mar. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.

[40] Gabriel J.X. Dance, Michael LaForgia & Nicholas Confessore, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. Times (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html.

[41] *E.g.,* Chris Hoofnagle, *Facebook in the Spotlight: Dataism vs. Privacy*, Jurist (Apr. 20, 2018), https://www.jurist.org/commentary/2018/04/chris-hoofnagle-facebook-dataism/.

[42] Moving Forward, Turn (Dec. 20, 2016), *available at* https://www.amobee.com/blog/moving-forward/.

In that spirit of building upon the GDPR and CCPA, CDT has put forward our own baseline privacy law discussion draft.[43] Our discussion draft and a section-by-section analysis are attached as appendices to these comments.

In short, our proposal (1) declares unfair certain data processing practices for secondary purposes, (2) requires reasonable security practices and transparency from companies, (3) builds on longstanding Fair Information Practice Principles (FIPPs) to grant affirmative access, correction, deletion, and portability rights to individuals, and (4) prevents advertising discrimination against protected classes and looks to the future of data protection regulation.

1. Privacy Protections Must Prohibit Generally Unfair Data Processing Practices

The Commission has inquired whether a federal data privacy framework ought to be based on the Fair Information Practice Principles (FIPPs). CDT has long reiterated our believe that the FIPPs can guide commercial data practices,[44] and their full incorporation into law has been a common demand of privacy and consumer advocates.[45] However, we could caution against an over-reliance on the FIPPs at the principle-level for governing current data flows and data-driven technologies. Companies are well aware of the FIPPs and are likely to assert that they have considered all relevant principles and determined their products, services, or data practices have struck the right balance.[46] The conversation our country is having now is because individuals fundamentally disagree with how companies have exercised the considerable discretion they are currently afforded. The Commission's goal must be to provide more concrete rules that rebalance routine data processing in a way that better protects individuals.

To the extent the FIPPs provide the foundational principles of a new privacy framework, we would encourage the FTC to address all of them. However, the FTC has historically distilled the FIPPs to prioritize notice to the detriment of the other principles.[47] Past commissioners have suggested that all privacy violations can be cast in terms of a "failure to disclose."[48] While this may be the predictable

---

[43] Federal privacy Legislation, Center for Democracy & Tech., *available at* https://cdt.org/campaign/federal-privacy-legislation/ (last visited Dec. 21, 2018).

[44] *See* CDT Info Injury Comments, *supra* note 1; Ctr. for Democracy & Tech., Recommendations for a Comprehensive Privacy Protection Framework (Feb. 4, 2011), https://cdt.org/insight/recommendations-for-a-comprehensive-privacy-protection-framework/.

[45] Public Interest Privacy Legislation Principles 1 (Nov. 13, 2018), *available at* https://cdt.org/blog/cdt-signs-onto-principles-for-privacy-legislation-calls-on-ntia-to-promote-robust-privacy-law-in-congress/.

[46] For example, data brokers have begun speaking not about privacy protections but rather "ethically-sourced" data, which ultimately just asks whether companies have obtained appropriate consents and offered certain notices. *See* Molly Hulefeld, *What is a chief data ethics officer, anyway?*, IAPP (Nov. 27, 2018), https://iapp.org/news/a/making-way-for-the-rise-of-the-chief-data-ethics-officer/.

[47] *See* Robert Gellman, Fair Information Practices: A Basic History 20-21 (Apr. 10, 2017), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

[48] J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Remarks before the Int'l Ass'n of Privacy Prof. 20 (2012), https://www.ftc.gov/sites/default/files/documents/public_statements/some-thoughts-evolving-nature-data-security-and-privacy-protection/121204privacyiapp.pdf.

result of the Commission's general reliance on its Section 5 deception authority to police privacy, it is an untenable position. As the NTIA acknowledged as part of its ongoing work to craft a privacy framework for the Trump administration, notice mandates result "primarily in long, legal, regulator-focused privacy policies and check boxes, which only help a very small number of users who choose to read these policies and make binary choices."[49]

Industry self-regulation often doubles down on this approach, relying heavily on "notice and choice" or some formulation of "user control" as a proxy for respecting individuals' privacy.[50] We have previously highlighted to the FTC our concerns with notice fatigue and "sticky" default settings.[51]

Instead of relying on notice and choice, CDT is calling on Congress to declare certain data processing activities as presumptively unfair. This aims to address the longstanding request of privacy advocates and scholars for the FTC explore its use of unfairness authority;[52] last year, the World Privacy Forum suggested the FTC use its existing authority "to define in more detail what constitutes unfairness," which "would go a long way to establish clearer standards for companies and produce better results for consumers."[53] Professor Dennis Hirsch has argued that constitutional doctrines of equal protection and due process, anti-discrimination laws, rules governing racial profiling, statutes such as the Genetic Information Nondiscrimination Act (GINA) that limit secondary uses of personal data, state laws limiting employer access to and use of employee social media postings, and the FTC's own established policies can inform whether uses of information are unfair.[54]

Though frequently minimized, often both by commentators and the FTC, public policy considerations play an important role in the existing Section 5 test for unfairness. CDT would enshrine in U.S. public

[49] 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.

[50] *See* Woodrow Hartzog, *The Case Against Idealising Control*, European Data Protection Law Review 4:4, 423 - 432 (2018). Google, for example, has called for a privacy framework that emphasizes "transparency, control, and choice." Written Testimony of Sundar Pichai, Chief Executive Officer, Google LLC Before the House Judiciary Committee Hearing on "Transparency & Accountability: Examining Google and its Data Collection, Use, and Filtering Practices" (Dec. 11, 2018), https://judiciary.house.gov/wp-content/uploads/2018/11/Pichai-Testimony.pdf.

[51] CDT Remediation Comments, *supra* note 1, at 5.

[52] *See* Letter from Consumer and Privacy Groups to the FTC, FTC 2017: 10 Steps for Protecting Consumers, Promoting Competition and Innovation (Feb. 15, 2017), https://epic.org/privacy/internet/ftc/EPIC-et-al-ltr-FTC-02-15-2017.pdf (recommending the FTC bring more actions under its unfairness authority); *see also* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 345-47 (2016).

[53] Comments of the World Privacy Forum to the Federal Trade Commission Regarding Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201, 5 (Aug. 20, 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0052-d-0039-155214.pdf (further calling for the FTC to "bring more cases that rely on unfair practices").

[54] Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345, 361 (2015).

policy that data processing that is (1) likely to be unexpected by the average person, (2) hard for individuals to avoid, and (3) hard to engage in with appropriate privacy safeguards should be viewed as unfair where they involve certain data repurposing.

Rather than a general data minimization prohibition, CDT has identified several specific data processing practices that warrant particular attention due to the factors above, as well as existing legal protections. These practices include:

- Biometric identification and verification
- Precise geospatial tracking
- Probabilistic tracking
- Tracking of children
- Disclosure of content and parties to communications
- Surreptitious audio and visual recording
- Secondary uses of health information

CDT proposes a relatively straightforward test: generally these practices are permissible if necessary to the product or service being offered but may not be collected, used or shared for other purposes. Very limited exceptions may be possible if they benefit the consumer and have been approved by a regulator.

Additionally, privacy self-management cannot address manipulative or discriminatory data practices. CDT would explicitly codify the enforcement lessons from deceptive practices like "dark patterns" that are designed to coerce or confuse users into providing their information. Discriminatory uses of data present further challenges. Ubiquitous data collection can be used in ways that systematically discriminate based on minority or protected classes such as race, age, gender, LGBTQ status, disability, or financial status. Data-driven discrimination can be completely opaque to the affected person and often goes unnoticed even by the discriminating party. This problem is vast and demands multiple legal and policy approaches. As we suggested to the FTC in earlier comments, certain targeted advertising seems to raise serious discrimination questions.[55]

2. Companies Must Have Affirmative Obligations to Protect Data and Provide Meaningful Information About Their Data Use

Entities that collect, use, and share data have a responsibility to safeguard it and prevent misuse. Nevertheless, the number of data breaches and security incidents continues to grow year over year. Companies do not have adequate incentives to properly invest in data security, often seeing regular

[55] Comments of the Center for Democracy & Technology re: FTC Hearings on Competition and Consumer Protection in the 21st Century, Question 9 (Aug. 20, 2018), https://cdt.org/files/2018/08/CDT-FTC-comments-9-8-20-18.pdf.

data breaches and security incidents as a cost of doing business.[56] CDT supports the Commission's longstanding calls for federal data security legislation, most recently reiterated before the Senate Commerce Committee.[57] Our discussion draft includes provisions that would require covered entities to adopt reasonable data security practices and engage in reasonable oversight of third parties with whom they share personal information. These obligations recognize the reality that participating in modern society often means ceding control of one's personal information. The entities we trust with our data should handle it with care.

Further, while notice requirements are not sufficient to protect user privacy, companies must provide more transparency about their data practices and material privacy mishaps in order for consumer advocates, privacy researchers, and the Federal Trade Commission to more effectively scrutinize covered entities on behalf of consumers. Some have argued, understandably, that privacy policies should be shorter and easier for users to understand. We should acknowledge the inherent tension is requiring disclosures that are *both* clear and comprehensive, which has produced arguably longer *and* vaguer disclosures.[58] Simplifying privacy policies can unintentionally reinforce the idea of privacy self-management while allowing companies to hide the details of their data processing. Considerable energy has been spent by the Commission, as well as by privacy researchers, to promote multi-layered notices, just-in-time notices, and other contextual disclosures,[59] but there is scant evidence that consumer awareness and understanding of privacy practices has increased. Our draft prioritizes detail and standardization over simplicity.

---

[56] Benjamin Dean, *Why Companies Have Little Incentive to Invest in Cybersecurity* (Mar. 4, 2015), http://www.theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570; *see also* Sasha Romanosky, *Cost of Cyber Incidents Not Large Compared with Other Business Losses; May Influence Responses by Businesses*, Rand (Sept. 20, 2016), https://www.rand.org/news/press/2016/09/20/index1.html.

[57] Prepared Statement of the Federal Trade Commission: "Oversight of the FTC," Before the Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security of the Committee on Commerce, Science, and Transportation, United States Senate (Nov. 27, 2018), https://www.ftc.gov/public-statements/2018/11/prepared-statement-federal-trade-commission-oversight-ftc-subcommittee.

[58] The FTC acknowledged as much in 2010. *See* Press Release, Fed. Trade Comm'n, FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010), https://www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers. There is a rich history of academic literature on the failure of the privacy policy. *See e.g.*, Fred Cate, *The Limits of Notice and Choice*, 8 IEEE SEC & PRIVACY 59, 59–62 (2010). Commentators continue to criticize the structure of privacy policies from both angles. *See e.g.*, Priya Kumar, *Privacy Policies and Their Lack of Clear Disclosure Regarding the Life Cycle of User Information* (2016), https://rankingdigitalrights.org/2017/01/06/companies-fail-privacy-policies/; Natasha Lomas & Romain Dillet, *Terms And Conditions Are The Biggest Lie of Our Industry*, TECHCRUNCH (Aug. 21, 2015), https://techcrunch.com/2015/08/21/agree-to-disagree/. The GDPR has accelerated these trends. Joanna Stern, *Those Privacy Policies Flooding Your Inbox? Print Them Out and They Span a Football Field*, WALL ST. J. (May 17, 2018), https://www.wsj.com/articles/privacy-policies-flooding-your-inbox-how-to-cut-through-the-gibberish-1526565342.

[59] FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES, *supra* note 10; *see also* Florian Schaub et al., A Design Space for Effective Privacy Notices (2015), *available at* https://www.ftc.gov/system/files/documents/public_comments/2015/10/00038-97832.pdf.

3. Affirmative Individual Rights to Information Are a Mandatory Component of any Privacy Framework

Provisions in the GDPR and CCPA that grant individuals the ability to access and delete personal information have ensured that these rights are basic requirements of any federal privacy framework. Individuals must have access to and, in some instances, the ability to correct their personal data held by companies. They should have the ability to delete and remove their data from services. The public should have detailed information about what data companies are collecting and with whom they share it. Many of these types of overarching privacy rights should be noncontroversial, and many companies already provide these rights under the GDPR -- and extend them to U.S. residents.[60]

Acknowledging that there are ongoing efforts to clarify how to operationalize data access[61] and portability,[62] CDT supports providing broad individual rights to data with tailored exceptions to account for technical feasibility, legitimate needs such as fraud detection and public interest research, and free expression rights. These rights should apply not only to information directly disclosed to a covered entity, but also to information inferred by the covered entity. Inferences can be more sensitive and relevant than the data individuals directly provide to a company, are often invisible to individuals and the public, and can be the basis for decisions that have significant effects on people's lives.[63]

4. U.S. Federal Privacy Law Must Be Forward-Looking and Address Emerging Informational Injuries

Applications of artificial intelligence and machine learning have been termed the "ultimate test for privacy" and have been an extensive focus of the GDPR,[64] yet are frequently dismissed in privacy conversations and debates. At the FTC's recent November hearing on privacy, big data, and competition, for example, panelists seemed to want to divorce "privacy" considerations from larger issues of discrimination and personal autonomy.[65] Similarly, we noted that the NTIA's recent call for comment on

---

[60] *E.g.*, Julie Brill, *Millions use Microsoft's GDPR privacy tools to control their data — including 2 million Americans*, Microsoft (Sept. 17, 2018), https://blogs.microsoft.com/on-the-issues/2018/09/17/millions-use-microsofts-gdpr-privacy-tools-to-control-their-data-including-2-million-americans/.

[61] The California Attorney General has stated his intentions to address the "verified access request" requirement in the CCPA.

[62] Data Transfer Project, https://datatransferproject.dev (last visited Dec. 20, 2018).

[63] *See* Office of Oversight & Investigations, Majority Staff, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Senate Commerce Committee (Dec. 18, 2013), https://www.commerce.senate.gov/public/_cache/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a/D5E458CDB663175E9D73231DF42EC040.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf.

[64] Eduardo Ustaran, *Is Artificial Intelligence the Ultimate Test for Privacy?*, Hogan Lovells (Mar. 2, 2018), https://www.hldataprotection.com/2018/03/articles/consumer-privacy/is-artificial-intelligence-the-ultimate-test-for-privacy/.

[65] Fed. Trade Comm'n, Transcript of FTC Hearing on Competition and Consumer Protection in the 21st Century, at 201 (Nov. 7, 2018),

an administration privacy framework ignored the problems posed by opaque and discriminatory algorithms. As Ryan Calo has noted, machine learning permits organizations "to derive the intimate from the available."[66]

As we detailed in comments to the FTC in August, this raises serious issues for data-driven practices ranging from eligibility determinations to targeted marketing. Studying these practices has been challenging because individual users don't know what offers they are excluded from seeing, and companies seldom, if ever, release the precise targeting parameters.[67] Behavioral or interest-based targeting categories can be proxies for sensitive characteristics even if they appear facially neutral. Some types of harmful targeting actually seek out minority groups rather than exclude them.

Our discussion draft directs the Commission to engage in studies and rulemaking to address advertising that is likely to result in unlawful discrimination. Such authority is also needed in light of elements in the GDPR that attempt to give individuals more rights with respect to "profiling" and "automated decisionmaking" practices.

Finally, the Commission has questioned whether there are gaps in existing U.S. privacy laws. While some have argued that the U.S. sectoral approach to privacy has merit and could, in fact, be ideal,[68] it clearly creates situations where individual Americans and companies are confused about where and when information is protected by a law -- and what protections or security standards apply in either situation. Health information, which the FTC considers especially sensitive, provides a dramatic illustration of this problem. The Health Insurance Portability and Accountability Act (HIPAA), for example, only applies to "covered entities" holding "protected health information," but information outside of this framework is governed by a mixture of other laws and self-regulatory guidance.[69] Separate privacy laws govern specific areas of the U.S. health-care system: student immunizations and other school health records are generally covered by the Family Educational Rights and Privacy Act (FERPA), which was enacted in 1974, when student records existed in physical file cabinets and not digital clouds. FERPA, in turn, intersects with and sometimes conflicts with the Children's Online Privacy Protection Act (COPPA), which does protect data, but only of children under the age of thirteen.

At minimum, companies are calling for additional guidance, but it is long past time to assess and update existing sectoral laws. Agencies have begun this process. Recently, HHS has begun to solicit input on

---

https://www.ftc.gov/system/files/documents/public_events/1418633/ftc_hearings_session_6_transcript_day_2_11-7-18.pdf.

[66] Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. Davis L. Rev. 399, 421 (2017).

[67] Upturn, Leveling the Platform: Real Transparency for Paid Messages on Facebook, at 16 (May 2018), https://www.teamupturn.org/static/reports/2018/facebook-ads/files/Upturn-Facebook-Ads-2018-05-08.pdf.

[68] Paul Schwartz, *Preemption and Privacy*, 118 Yale L.J. 902 (2008).

[69] Network Advertising Initiative, *Another Look at NAI's High Standards for Health Data* (July 1, 2014), https://www.networkadvertising.org/blog/another-look-nais-high-standards-health-data.

revising the HIPAA Privacy Rule,[70] while emerging financial technologies (fintech) have caused both the Treasury Department and the Consumer Financial Protection Bureau to explore data governance and security issues in financial data access.[71] Any meaningful federal privacy framework will include a mechanism by which to (1) identify inconsistencies and inadequate protections in existing federal law, (2) offer recommendations to amend federal laws in light of changing technological and economic trends, and (3) detail the enforcement activities of federal (and state) regulators. Presumably the FTC would be at the vanguard of such an effort.

--

The Commission has asked a series of important questions about how best to regulate our technology driven society and its impact on our privacy, personal autonomy, and opportunities, and we thank them for focusing attention on these important issues. CDT will continue to advocate for a legislative solution to these challenges, and we would encourage the Commission, through its ongoing hearings on privacy matters, to discuss and propose concrete guardrails to protect individuals' information from misuse by commercial interests.

Thank you for the opportunity to submit comments and please do not hesitate to contact us with further questions.

Sincerely,

Joseph Jerome
Policy Counsel, Privacy & Data Project

Michelle Richardson,
Director, Privacy & Data Project

Enclosures:

- CDT Federal Baseline Privacy Legislation Discussion Draft
- Section-by-Section Analysis and Explanation

[70] Office of Civil Rights, U.S. Dep't of Health & Human Servs., Request for Information on Modifying HIPAA Rules To Improve Coordinated Care, 83 Fed. Reg. 64302 (Dec. 14, 2018), https://www.federalregister.gov/documents/2018/12/14/2018-27162/request-for-information-on-modifying-hipaa-rules-to-improve-coordinated-care.

[71] U.S. Dep't of the Treasury, A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation (2018), https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf; Press Release, Consumer Financial Protection Bureau, CFPB Outlines Principles For Consumer-Authorized Financial Data Sharing and Aggregation (Oct. 18, 2017), https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-principles-consumer-authorized-financial-data-sharing-and-aggregation/.

CENTER FOR DEMOCRACY & TECHNOLOGY

Section-by-Section Analysis and Explanation

Section 1: Definitions

- Includes definitions for terms in the bill, most notably:
  - **Defines "personal information" broadly** to include any information linked or reasonably linkable by the covered entity to a specific covered person or consumer device, but excludes employee information from coverage. The individual rights in Section 2 do not require companies to re-identify information or convert non-personal information to personal information.
  - **Defines "covered entities" broadly** as any person or business that processes personal information in or affecting interstate commerce. Covered entities do not include government entities or natural persons, except for natural persons acting in a non-de-minimis commercial capacity.
  - **Defines "health information" to include three types of different data:** (1) information related to health conditions or the provision of health care, (2) information processed in the course of providing health or wellness services, or (3) information derived from a testing or examination of the body. Empowers the Federal Trade Commission (FTC) to further define "health information."
  - **Defines third parties to include corporate affiliates** if they hold themselves out as a separate entity such that reasonable individuals would not expect the two companies to be related.

Section 2: Individual Rights with Respect to Personal Information

- **Establishes affirmative rights for individuals** with respect to personal information.
  - **Right to Access and Correction:** Permits individuals to access both their personal information and the names of third parties to which personal information is sold or licensed. Allows individuals to dispute the accuracy of their personal information in certain circumstances such as where it is being used for an eligibility determination for credit, insurance, housing, employment or educational opportunity, or is health information.
  - **Right to Data Portability:** Permits individuals to transmit or transfer their personal information from a business, where appropriate, or lets individuals download personal information for their own use. Calls for the National Institute of Standards and Technology (NIST) to convene a working group to advance data portability.
  - **Right to Deletion:** Permits individuals to delete their personal information, which businesses may not make unreasonably difficult to do.
- **Provides reasonable exceptions for businesses** to deny these affirmative rights where individuals cannot confirm their identity, other legal limits are in place, or a covered entity makes a determination that exercising these rights creates a legitimate risk to another individual. Deletion and correction rights are also limited where a covered entity must retain

information for traditional business and security purposes, or deletion would interfere with ongoing research in the public interest.
- **Clarifies that de-identified data need not be re-identified** or "converted" back to personal information in order to affect these rights.

Section 3: Obligations of Covered Entities with Respect to Personal Information

- **Requires companies to put in place complaint mechanisms** for individuals to inquire about their privacy rights and to respond within 30 days.
- **Establishes clear rules for data security** by granting authority to the FTC to enact rules that are tailored to the business's practices, the type of personal information, and current state of the art in safeguards.
- **Requires companies to certify their privacy oversight policies** and disclose any material data security of privacy incidents. Requires companies to provide clear notice to individuals of their rights under this framework.
- **Addresses third-party data sharing** by requiring companies that license or sell personal information to third parties to contractually bind the third parties to the same privacy commitments as the company that collected the information. Companies are also required to exercise reasonable oversight of these contracts, take action against any company that violates these rules, and disclose those violations.
- **Addresses the lack of data broker transparency** by directing the FTC to create a centralized opt-out registry of data brokers.

Section 4: Deceptive Data Processing Practices

- **Codifies existing FTC enforcement precedent** by prohibiting misleading statements and material omissions regarding a company's privacy practices.

Section 5: Unfair Data Processing Practices

- **Identifies certain data practices as presumptively unfair** to individuals when those activities are **not required** for or **do not add to the functionality** of products, services, or specific features unless a limited exception applies or the FTC has reviewed the practice. For example, a flashlight application could no longer collect and use an individual's precise geolocation.
    - **Limits all processing of biometric information**, including facial recognition templates, for identifying an individual or verifying their identity.
    - **Limits all processing of precise location information** that is generated by consumer devices. Location information is defined to include precise geospatial data that generates latitude-longitude coordinates with an accuracy level below 1,500 feet.
    - **Limits "cross-device tracking,"** which is the use probabilistic methods like usage patterns to attribute specific consumer devices to specific individuals. Covered entities may still link devices through a common account or login.

    - **Limits the disclosure to third parties of information collected from children under the age of 13** and its use for targeted marketing.
    - **Limits the licensing or sale of personal information relating to the contents of communications or the parties to communications.** Contents are defined to have the same meaning as they do under the Electronic Communications Privacy Act. Parties to communications include the sender and recipient or destination of a communication. The definition of parties excludes subscriber information, such as contact information disclosed for the purpose of setting up an account.
    - **Limits the retention, use, or disclosure of information collected from microphones and cameras** of consumer devices.
    - **Limits processing of health information.** Recognizing that the line where information becomes "health" information varies, several collection- and use-based definitions are provided, and the FTC is afforded the flexibility to further define health information.
- **Provides a limited set of exceptions** to this broad prohibition, including (1) security and fraud, (2) imminent danger, (3) repairing errors in intended functionality, (4) research in the public interest, and (5) legal compliance. Importantly, providing a consent checkbox does not serve to get around the general prohibitions.
- **Directs the FTC to write rules within two years to create a process by which a company can seek an exception to these prohibitions**.

Section 6: Unfair Targeted Advertising Practices

- **Addresses unlawful discrimination in targeted advertising** by giving the FTC the authority to issue rules that restrict harmful targeted advertising practices that are likely to result in unlawful discrimination, including under existing civil rights laws. This provision encourages further research and investigation into the effects of algorithms and tools provided by social media services, ad networks, and data brokers to microtarget advertising online.

Section 7: Enforcement

- **Provides for joint enforcement by the FTC and state Attorneys General,** with the FTC having the ability to preempt action by states.
- Creates new civil penalties against companies that violate this framework.

Section 8: Additional Personnel in the Bureau of Consumer Protection

- **Boosts legal, privacy, and technical expertise within government** by requiring the FTC to hire additional personnel in the Bureau of Consumer Protection to police corporate privacy violations.

Section 9: Effective Date

- **Gives companies a two-year window** to provide sufficient lead time to meet the framework's requirements.

Section 10: Relation to Other Privacy & Security Laws

- **Preempts state laws that are focused primarily on data privacy** such as the **California Consumer Privacy Act** and the **Illinois Biometric Information Privacy Act**. Does not preempt state data breach notification requirements or consumer protection laws of general applicability, such as state unfair and deceptive acts or practices (UDAP) statutes that permit actions against fraud or other general consumer harms.
- **Affirms that this framework does not limit existing federal civil rights laws** but exists alongside most existing federal privacy laws.
- **Transfers privacy and security enforcement responsibilities** from the Federal Communications Commission (FCC) to the FTC for businesses regulated under the Communications Act of 1934. Brings nonprofits under the purview of the FTC for the purposes of this bill.
- **Requires regular reporting on how best to update or improve existing privacy laws** like the HIPAA Privacy Rule or the privacy provisions in GLBA. The Government Accountability Office (GAO) is assigned responsibility to undertake periodic studies to identify inconsistencies with the privacy protections in this framework.

CENTER FOR DEMOCRACY & TECHNOLOGY

SEC. 1: DEFINITIONS

(1) PERSONAL INFORMATION. -- The term "personal information" means any information held by a covered entity, regardless of how the information is collected, inferred, created, or obtained, that is linked or reasonably linkable by the covered entity to a specific covered person or consumer device. Data is linked or reasonably linkable to a covered person or consumer device if it can be used on its own or in combination with other information held by or readily accessible to the covered entity to identify a covered person or consumer device.

(A) "Personal information" shall not include information about employees or employment status collected or used by an employer pursuant to an employer-employee relationship.

(2) PERSONAL HEALTH INFORMATION. -- "Personal Health information" includes personal information that:

(A) Relates to the physical or mental health or condition of a covered person or the provision of health care to a covered person;

(B) Is processed for the purpose or in the course of providing health or wellness services; or

(C) Is derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples.

(3) COMMISSION. -- The term "Commission" means the Federal Trade Commission.

(4) CONSUMER DEVICE. -- The term "consumer device" means any electronic device capable of transmitting or receiving information designed to be used by a covered person for non-commercial purposes.

(5) COVERED ENTITY. -- The term "covered entity" means a person or business entity that as part of its activities processes personal information in or affecting interstate commerce. Such term does not include:

(A) the federal Government, the Government of any State, Territory, or Federal District; the Government of any Indian tribe; or any political subdivision, department, agency, component entity, or instrumentality thereof;

(B) any employee, officer, agent, contractor, or organization working on behalf of such an entity described in subparagraph (A), with regard to data processed on behalf of such entity; or

(C) a natural person, unless acting in a non-de-minimis commercial capacity.

(6) COVERED PERSON. -- The term "covered person" is a natural person residing in the United States.

(7) DATA BROKER. -- The term "data broker" means a covered entity, or affiliate or subsidiary of a covered entity, that primarily collects and sells or licenses to any other party with whom the covered entity does not have a direct relationship, the personal information of covered persons for the third party's own purposes.

(8) PROCESSING. -- The term "processing" means any operation or set of operations performed on personal information including collection, creation, organization, structuring, storage, retaining, using, disclosing, sharing, transmitting, selling, licensing, disposing of, or otherwise handling personal information.

(9) SERVICE PROVIDER. -- The term "service provider" means a person or business entity that processes personal information only on behalf of and at the direction of a covered entity.

(10) THIRD PARTY. -- The term "third party" means a covered entity that receives personal information from or transfers personal information to another covered entity and is not a service provider of the other covered entity. The term "third party" includes any affiliate or corporate entity that holds itself out to the public as separate from the other covered entity, such that an individual acting reasonably under the circumstances would not expect it to be related to the other covered entity or to have access to personal information provided to the other covered entity.

SEC. 2: INDIVIDUAL RIGHTS WITH RESPECT TO PERSONAL INFORMATION

(1) RIGHT TO ACCESS AND CORRECTION. --
- (A) Upon request, a covered entity shall provide to a covered person reasonable access to personal information the covered entity retains and the names of third parties to whom personal information is sold or licensed.
- (B) A covered person shall have, upon request, the right to dispute the accuracy or completeness of:
  - (i) Personal health information; and
  - (ii) Personal information processed for the purpose of:
    - (a) Making determinations about a covered person's educational opportunities; or

(b) Determining eligibility for credit, insurance, housing, or employment by a covered entity.

(C) A covered entity shall make available a reasonably accessible, conspicuous, and easy-to-use means for a covered person to exercise their right to access and correction. If a covered entity has a direct relationship with a covered person, it shall offer such means at least via the same medium(s) that a covered person routinely uses to interact with the covered entity.

(2) RIGHT TO DATA PORTABILITY. --

(A) Where technically feasible, a covered entity shall make available a reasonable means for a covered person to transmit or transfer personal information about the covered person retained by the covered entity to another covered entity in a structured, standardized, and machine-readable interoperable format, or otherwise download personal information for the covered person's own use.

(B) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CONVENING ON PORTABILITY STANDARDS. -- Not later than 1 year after the date of enactment of this Act, the Department of Commerce shall establish a working group at the National Institute of Standards and Technology to promote common frameworks and cooperation to foster the interoperable portability of personal information. The group shall prioritize addressing reasonable limitations on portability. Such group should include equal numbers of industry representatives, public interest representatives, and technical experts.

(3) RIGHT TO DELETION. --

(A) Upon request, a covered entity that retains personal information shall make available a reasonable means for a covered person to delete personal information. Covered entities may not make it unreasonably difficult for an individual to request such deletion.

(4) EXCEPTIONS. --

(A) A covered entity may decline to provide such access under subsection (1) and (2) if:

(i) A covered person cannot reasonably document or confirm his or her identity to the covered entity;

(ii) Such access is limited by law, legally recognized privilege, or other legal obligation;

(iii) A covered entity makes an individualized determination that fulfilling this request would create a legitimate risk to the privacy,

security, safety, free expression or other rights of an individual other than the covered person or the covered entity.

(B) A covered entity shall not be required to correct or delete personal information under subsections (1) and (3) respectively if:

(i) A covered person cannot reasonably document or confirm his or her identity to the covered entity;

(ii) Such correction or deletion request is limited by law, legally recognized privilege, or other legal obligation;

(iii) A covered entity makes an individualized determination that fulfilling such request would create a legitimate risk to the privacy, security, safety, free expression or other rights of an individual other than the covered person or the covered entity;

(iv) Retention of the information is necessary to:

(a) Complete the transaction for which the personal information was collected, provide a product or service affirmatively requested by a covered person, or otherwise necessary to perform a contract, including billing, financial reporting, and accounting;

(b) Detect or prevent security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for such activity;

(c) Identify and repair errors that impair existing intended functionality, or to ensure a product or service functions as intended; or

(v) Personal information is used in public or peer-reviewed scientific, medical, historical, or statistical research in the public interest that adheres to commonly accepted ethical standards or laws, with informed consent. In order to preempt a deletion request, the research must already be in progress at the time when deletion is requested.

(5) DENIAL OF REQUEST TO EXERCISE AN INDIVIDUAL RIGHT. -- If a covered entity denies a request by a covered person to exercise that person's right to access, correction, or deletion, the covered entity shall inform the covered person without undue delay, but no longer than 30 days, of the reasons for not fulfilling such request and any rights the covered individual may have to appeal the decision of the covered entity.

(6) FEES TO EXERCISE AN INDIVIDUAL RIGHT. -- A covered entity may not charge a fee to a covered person for exercising a right under Section 2 of this Act, unless such request is unfounded or excessive in which case a covered entity may

charge a reasonable fee for the administrative costs of complying with the request.

(7) RULE OF CONSTRUCTION. -- Nothing in this section shall be interpreted to require a covered entity to take an action that would convert information that is not personal information into personal information.

SEC. 3: OBLIGATIONS OF COVERED ENTITIES WITH RESPECT TO PERSONAL INFORMATION

(1) REDRESS. --

(A) A covered entity shall provide a reasonably accessible, conspicuous, and easy-to-use means for a covered person to make a complaint or inquiry regarding a covered entity's policies and procedures required by this Act. A covered entity shall be required to respond to a covered person's complaint or inquiry submitted via the established process without undue delay, but no longer than 30 days, to provide a response explaining what the outcome of that complaint or inquiry is, and to provide information about how to contact state Attorneys General and the Commission.

(2) SECURITY. --

(A) A covered entity shall establish and implement reasonable policies, practices, and procedures regarding information security practices for the protection of personal information taking into consideration --

(i) the nature, scope, and complexity of the activities engaged in by such covered entity;

(ii) the sensitivity of any personal information at issue;

(iii) the current state of the art in administrative, technical, and physical safeguards for protecting such information; and

(iv) the cost of implementing such administrative, technical, and physical safeguards.

(B) REQUIREMENTS. -- The policies, practices, and procedures required in subpart (A) of this section must include the following:

(i) A written security policy with respect to the processing of such personal information.

(ii) The identification of an officer or other individual as the point of contact with responsibility for the management of information security.

(iii) A process for identifying and assessing reasonably foreseeable security vulnerabilities in the system or systems maintained by such covered entity that contains such personal information, which shall

include regular monitoring for vulnerabilities and a breach of security of such system or systems.

(iv) A process for taking action designed to mitigate against vulnerabilities identified in the process required by subparagraph (iii), which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software, or for regularly testing or otherwise monitoring the effectiveness of the existing safeguards.

(v) A process for determining if personal information is no longer needed and disposing of personal information by shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such personal information permanently unreadable or indecipherable.

(vi) A process for overseeing persons who have access to personal information, including through network-connected devices.

(vii) A process for employee training and supervision for implementation of the policies, practices, and procedures required by this subsection.

(viii) A written plan or protocol for internal and public response in the event of a breach of security.

(C) REGULATIONS.—Not later than 2 years after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to implement this section.

(3) LIMITS ON THIRD PARTIES AND SERVICE PROVIDERS. --

(A) THIRD PARTIES. -- A covered entity shall not sell or license personal information it holds to a third party unless that third party is contractually bound to meet the same privacy and security obligations as the covered entity under this Act and any additional obligations to which the covered entity has publicly committed. A covered entity shall exercise reasonable oversight and take reasonable actions to ensure compliance with such contractual provisions.

(i) A covered entity that sells or licenses access to personal information to third parties shall be obligated to limit access to and seek certification of destruction of personal information if it obtains actual knowledge that another covered entity has materially violated the requirements of this Act. Such violations must be disclosed in the disclosures required in subsection (4), subpart (B).

(B) SERVICE PROVIDERS. -- A covered entity may not share or disclose personal information to a service provider unless the covered entity enters into a contractual agreement with the service provider that prohibits the

service provider from processing the personal information for any purpose other than the purposes for which the covered entity shared such personal information with the service provider. A service provider may not sell or license personal information provided by a covered entity. A covered entity shall exercise reasonable oversight and take reasonable actions to ensure compliance with such contractual provisions.

(4) DISCLOSURES. --

(A) INFORMATION TO COVERED PERSONS. --

(i) A covered entity shall make available, in reasonably clear, easily understandable, timely and visually prominent machine-readable format, information about the following:

(a) The types of personal information that the covered entity collects and the names of the third parties, including affiliates to whom the covered entity sells or licenses personal information;

(b) The general purposes for which the covered entity collects and uses personal information, including disclosure as to whether and how the covered entity customizes products or services or changes the prices of products or services based, in whole or in part, on a covered person's personal information;

(c) A description of how the covered entity provides individual rights as enumerated in this Act;

(d) A description of the controls and mechanisms, including methods of de-identifying personal information, the covered entity uses or makes available to covered persons to limit the collection, use, disclosure, or other processing of personal information;

(e) A description of the process by which the covered entity will notify individuals of material changes to its data policies; and

(f) The effective date of the disclosure.

(B) PERIODIC PRIVACY PROTECTION DISCLOSURES. --

(i) A covered entity shall be required to publish a disclosure at least annually, and prior to any material change, that includes:

(a) a list of purposes for which the covered entity processes personal information, including disclosure as to whether and how the covered entity customizes products or services or changes the prices of products or services based, in whole or in part, on a covered person's personal information;

(b) an assessment of the covered entity's approach to mitigating privacy risks, including:
  i) the designation of an employee charged with monitoring the covered entity's privacy practices covered by this Act;
  ii) the processes by which employees of a covered entity are educated and trained on data processing obligations;
  iii) the processes and procedures by which a covered entity audits, monitors, and addresses privacy risks;
  iv) a data retention policy that details how long personal information is retained in days, months, or years, or a disclosure that such information is retained indefinitely or permanently; and
  v) a summary of the security policies, practices, and procedures adopted pursuant to subsection (2).

(c) any material changes to the covered entity's policies or practices related to data processing and privacy since prior disclosure; and

(d) any security incidents or violations of the company's security about which the covered entity was required by law to provide notice to any individual located within the United States and privacy programs, including violations by third parties, and a general description of the covered entity's response.

(ii) A corporate officer of the covered entity must certify the information contained in the annual reports. A corporate officer includes one of the named executive officers under Item 402 of Regulation S-K under the Securities Act of 1933, the chief privacy officer (or equivalent thereof), or the chief information security officers (or equivalent thereof) of the covered entity.

(iii) The corporate officer must certify that:

(a) They have reviewed the disclosures;

(b) Based on their knowledge, the disclosures do not contain any untrue statement of fact or omission of a material fact necessary in order to make the statements not misleading with respect to the policies or practices covered in the report;

(c) They are responsible for establishing, maintaining and regularly evaluating the effectiveness of the covered entity's internal information security and privacy controls; and

(d) They have included information in the disclosure sufficient to understand any significant changes in the covered entity's internal information security and privacy controls.

(iv) The disclosures required by this subsection may be used to supplement the information provided to covered persons pursuant to the previous subsection, but shall not be sufficient to satisfy that subsection.

(v) EXCEPTION. -- This section does not apply to covered entities that process the personal information of 50,000 or fewer covered persons a year.

(C) DATA BROKERS. --

(i) The Commission shall facilitate or create an accessible online mechanism for individuals to identify data brokers. A covered entity which is a data broker shall be required to register with the Commission and provide information into their sources of personal information and how individuals may exercise their individual rights with respect to data brokers.

SEC. 4: DECEPTIVE DATA PROCESSING PRACTICES

(1) It shall be an unlawful for covered entities to make material misrepresentations with respect to the processing of personal information.

(A) MATERIALITY. -- A representation is material if it is likely to affect a reasonable person's conduct or decision with regard to a product or service. Express statements are presumptively material.

(2) A misrepresentation with respect to the processing of personal information includes but is not limited to:

(A) Notices, settings, interfaces, or other representations likely to mislead consumers as to how their personal information is being collected, retained, used, repurposed, shared, sold, or otherwise processed;

(B) The use of false pretenses, fraudulent statements, or other misrepresentations to induce the disclosure of personal information; and

(C) Misleading omission of material information about the processing of personal information.

(i) A misleading omission occurs when qualifying information necessary to prevent a practice, claim, representation, or reasonable expectation or belief from being misleading is not disclosed.

(3) When evaluating whether a representation is misleading, the Commission shall consider the totality of the covered entity's relevant representations from the

perspective of a reasonable consumer under the circumstances. When representations are targeted to a specific audience, the Commission shall evaluate the representations from the perspective of a reasonable member of that group.

(4) RULE OF CONSTRUCTION. -- Nothing in this section shall be construed to limit the Commission's authority to enforce against unfair and deceptive practices or to limit the authority of any federal agency or state to enforce any civil rights law, regulation, or requirement.

SEC. 5: UNFAIR DATA PROCESSING PRACTICES

(1) It shall be unlawful for a covered entity to engage in the following data processing practices when those practices are not required to provide or add to the functionality of the product, service, or specific feature that a covered person has requested.

(A) EXCEPTIONS. -- Not later than 2 years after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to implement procedures by which covered entities may petition the Commission for an exception to these prohibitions.

(2) BIOMETRIC INFORMATION TRACKING. -- The processing of biometric information to identify a covered person, or to verify a covered person's identity.

(A) BIOMETRIC INFORMATION. -- “Biometric information” means any personal information generated from the measurement or specific technological processing of an individual’s unique biological, physical, or physiological characteristics. Biometric information includes measurements of, but is not limited to, fingerprints, voice prints, iris scans, facial characteristics, identifying DNA (deoxyribonucleic acid) information, or other unique biological characteristics, including any mathematical code or algorithmic model generated or extracted from measurements of these characteristics. Biometric information does not include writing samples, written signatures, photographs, demographic data or physical descriptions such as height, weight, hair color, or eye color.

(3) PRECISE GEOSPATIAL INFORMATION TRACKING. -- The processing of precise geospatial information generated by a consumer device.

(A) PRECISE GEOSPATIAL INFORMATION. -- “Precise Geospatial Information” means information derived from a consumer device through any technology that is capable of determining with specificity the spatial

location of a person or device, such as latitude-longitude coordinates with an accuracy level of below 1,750 feet provided by GPS, or triangulated location provided by network radios or beacons such as Wi-Fi, or other technologies and inferences, provided however that it does not include information that is or will be altered prior to subsequent processing such that it cannot be determined with specificity the physical location of an individual or device.

(4) PROBABILISTIC CROSS-DEVICE TRACKING. -- The use of probabilistic methods, such as algorithms and usage patterns, to attribute a consumer device to a specific covered person.

(A) Information derived from probabilistic cross-device tracking for security, fraud detection, or other permissible purposes enumerated in subsection (9) shall not be used for any other purpose not enumerated in subsection (9) or otherwise required or permitted by law.

(5) TRACKING OF CHILDREN UNDER THE AGE OF 13. -- The disclosure of personal information collected from a child under 13 to third parties, and the use of such personal information for targeted advertising purposes, where a covered entity has actual knowledge that it is collecting personal information from a child or such information is collected from services, products, or specific features directed to children under the age of 13.

(6) CONTENT OF AND PARTIES TO COMMUNICATIONS. -- The licensing or sale to third parties of personal information relating to the contents of communications or the parties to communications.

(A) CONTENTS OF COMMUNICATIONS. -- “Content of communications” includes any part of the substance, purport, or meaning of a communication. Examples of contents include the text of an email or instant message; the video, webpage, application, or other information viewed or requested by a covered person; and the contents of a voice command from a covered person to a consumer device.

(B) PARTIES TO COMMUNICATIONS. -- “Parties to communications” means records or logs revealing the sender and recipient or destination of an electronic communication or telephone call.

(i) EXCEPTION.-- This section does not include subscriber information, which is contact information provided by a covered person to the covered entity to establish or maintain an account or communication channel.

(7) AUDIO AND VISUAL RECORDING. -- The retention, use, or disclosure to a third party of personal information or communications collected through the microphone or camera of a consumer device.

(8) HEALTH INFORMATION. -- The processing of personal health information.

(D) The Commission may by regulation promulgated under section 553 of title 5, United States Code, further define "health information," taking into consideration the reasonable expectations of an covered person and the adverse effect that a covered person may experience if such information is processed.

(9) EXCEPTIONS. -- Nothing in this section shall limit covered entities from engaging in these practices when necessary and solely for purposes of

(E) detecting and preventing security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity; or prosecuting those responsible for that activity;

(F) preventing imminent danger to the personal safety of an individual or group of individuals;

(G) identifying or repairing errors that impair existing intended functionality;

(H) engaging in public or peer reviewed scientific, medical, historical, or statistical research in the public interest that adheres to commonly accepted ethical standards or laws, with informed consent;

(I) complying with a Federal, State, or local law, rule, or other applicable legal requirement, including disclosures pursuant to a court order, subpoena, summons, or other properly executed compulsory process; and

(J) any other exception specified by the Commission pursuant to Section 5(1)(A) of this Act.

(11) RULE OF CONSTRUCTION. -- Nothing in this section shall be construed to limit the Commission's authority to enforce against unfair and deceptive practices or to limit the authority of any federal agency or state to enforce any civil rights law, regulation, or requirement.

SEC. 6: UNFAIR TARGETED ADVERTISING PRACTICES

FEDERAL TRADE COMMISSION RULEMAKING ON UNFAIR TARGETED ADVERTISING PRACTICES. --

(1) The Commission shall promulgate rules under section 553 of title 5, United States Code, to define and prohibit unfair targeted advertising practices, including but

not limited to practices that are likely to result in unlawful discrimination. In promulgating these rules, the Commission shall consider:

(A) Established public policy, such as civil rights laws, that can guide the Commission's determinations of what constitutes an unfair targeted advertising practice;
(B) The tools made available to, developed by, or used by advertisers to target advertisements online;
(C) The actual targeted advertising practices engaged in by advertisers and other covered entities;
(D) The effects of algorithms on the audiences reached by targeted advertisements;
(E) Methodologies for measuring discriminatory effects of targeted advertising;
(F) any relevant results of studies measuring discrimination, including discriminatory effect, in targeted advertising; and
(G) The role of all actors in the digital advertising ecosystem, including advertisers; websites and applications that carry targeted advertisements, including but not limited to social media services; advertising networks; and data brokers.

(2) RULE OF CONSTRUCTION. -- Nothing in this section shall be construed to limit the Federal Trade Commission's authority to enforce against unfair and deceptive practices or to limit the authority of any federal agency or state to enforce any civil rights law, regulation, or requirement.

SEC. 7: ENFORCEMENT

(1) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION. --
(A) UNFAIR OR DECEPTIVE ACTS OR PRACTICES. -- A violation of this Act shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act.
(B) POWERS OF COMMISSION. -- The Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as through all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act, except where granted rulemaking authority under section 553 of title 5, United States Code herein.
(C) COMMON CARRIERS AND NONPROFIT ORGANIZATIONS. -- Notwithstanding Sections 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) or any jurisdictional limitation of the Commission, the Commission shall also enforce this Act with respect to:

(i) Common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.); and
(ii) Organizations not organized to carry on business for their own profit or that of their members.

(2) ENFORCEMENT BY STATE ATTORNEYS GENERAL. --
(A) CIVIL ACTION. -- In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is adversely affected by any person who violates this Act, the attorney general of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States --
(i) to enjoin further violation of this Act by the defendant;
(ii) to compel compliance with this Act; or
(iii) for violations of subsections of this Act to obtain civil penalties in the amount determined under subsection (3).
(B) RIGHTS OF FEDERAL TRADE COMMISION. -- The attorney general of a State shall notify the Federal Trade Commission in writing of any civil action under subsection (2), subpart (A), prior to initiating such civil action. Upon receiving notice with respect to a civil action, the Federal Trade Commission may --
(i) intervene in such action; and
(ii) upon intervening --
(a) be heard on all matters arising in such civil action; and
(b) file petitions for appeal of a decision in such action.
(C) PREEMPTIVE ACTION BY FEDERAL TRADE COMMISSION. -- If the Federal Trade Commission institutes a civil action for violation of this Act or a regulation promulgated under this Act, no attorney general of a State may bring a civil action against any defendant named in the complaint of the Commission for violation of this Act or a regulation promulgated under this Act that is alleged in such complaint.

(3) CIVIL PENALTIES. -- The Commission or State Attorneys General may commence a civil action to recover a civil penalty in a district court of the United States against any covered entity or service provider that violates this Act.
(A) IN GENERAL. -- A violation of this Act shall be subject to a civil penalty in an amount that is not greater than $16,500 per covered person for whom the covered entity processed personal information in violation of this Act.
(B) DETERMINATION. -- Penalties shall be calculated based on the number of individuals whose personal information was affected by a violation;

however, penalties shall be proportionate to the severity of the violation as well as to the size and revenues of the covered entity.

SEC. 8: ADDITIONAL PERSONNEL IN THE BUREAU OF CONSUMER PROTECTION

(1) IN GENERAL. -- Notwithstanding any other provision of law, the Director of the Bureau of Consumer Protection of the Commission shall appoint--

(A) 100 additional personnel in the Division of Privacy and Identity Protection of the Bureau of Consumer Protection, of which no fewer than 25 personnel will be added to the Office of Technology Research and Investigation; and no fewer than 25 additional personnel in the Division of Enforcement of the Bureau of Consumer Protection.

(2) AUTHORIZATION OF APPROPRIATIONS. -- There is to be authorized to be appropriated to the Director of the Bureau of Consumer Protection such sums as may be necessary to carry out this section.

SEC. 9: EFFECTIVE DATE

(1) The provisions of this Act that apply to covered entities shall apply beginning on or after the date that is 2 years from the date of enactment of this Act.

SEC. 10: RELATION TO OTHER PRIVACY & SECURITY LAWS

(1) SEVERABILITY. -- If any provision of this Act, or the application thereof to any covered entity or covered person, is held unconstitutional or otherwise invalid, the validity of the remainder of the Act and the application of such provision to other covered entities and covered persons shall not be affected thereby.

(2) PREEMPTION. -- This Act supersedes any provision of a statute, regulation, requirement, or rule of a State or political subdivision of a State, with respect to those entities covered by this Act, that requires covered entities to implement requirements with respect to the processing of personal information addressed in this Act.

(A) EXCEPTIONS.-- This law does not preempt laws that address the collection, use, or disclosure of health information covered by the Health Insurance Portability and Accountability Act or financial information covered by Gramm-Leach-Bliley Act.

(B) RULE OF CONSTRUCTION. -- This Act shall not be construed to preempt the applicability of the following laws, rules, regulations or requirements:
- (i) Consumer protection laws of general applicability unrelated to privacy or security;
- (ii) Civil rights laws;
- (iii) Laws that govern the privacy rights or other protections of employees and employee information;
- (iv) Laws that address notification requirements in the event of a data breach;
- (v) Trespass, contract, or tort law;
- (vi) Criminal laws governing fraud, unauthorized access to information, malicious behavior, and similar provisions, and laws of criminal procedure; and
- (vii) Public safety or sector specific laws unrelated to privacy or security.

(3) GOVERNMENT ACCOUNTABILITY OFFICE STUDY AND REPORT. --

(A) Not later than 3 years after the date of effective date of this Act, and every 3 years thereafter, the Comptroller General of the United States shall submit to the President and Congress a report that surveys federal privacy and security laws, including any legislative or executive recommendations, that:
- (i) Identifies inconsistencies between this Act and those enumerated laws in subsection (4);
- (ii) Provides recommendations for how to amend federal privacy and security laws in light of changing technological and economic trends; and
- (iii) Details the privacy and security enforcement activities of the Commission and other federal agencies.

(4) EFFECT ON OTHER FEDERAL LAWS. --

(A) Nothing in this Act may be construed to modify, limit, or supersede the operation of privacy or security provisions in the following Federal laws:
- (i) Section 552a of title 5, United States Code (commonly known as the Privacy Act of 1974);
- (ii) The Right to Financial Privacy Act of 1978 (12 U.S.C. § 3401 et seq.);
- (iii) The Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);
- (iv) The Fair Debt Collection Practices Act (15 U.S.C. § 1692 et seq.);
- (v) Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.);
- (vi) Chapters 119, 123, 206, and 121 of Title 18, United States Code;
- (vii) Section 2710 of Title 18, United States Code;

(viii) Sections 444 and 445 of the General Education Provisions Act (20 U.S.C. §§ 1232g, 1232h), commonly known as the "Family Educational Rights and Privacy Act of 1974" and the "Protection of Pupil Rights Amendment," respectively;
(ix) Sections 5701 and 7332 of Title 38, United States Code;
(x) The Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d-2 et seq.);
(xi) The Privacy Protection Act of 1980 (42 U.S.C. § 2000aa et seq.);
(xii) The provisions of part C of title XI of the Social Security Act, section 264 of the Health Insurance Portability and Accountability Act of 1996, and subtitle D of title IV of the Health Information Technology for Economic and Clinical Health Act, and regulations under such provisions;
(xiii) The E-Government Act of 2002 (44 U.S.C. § 101 et seq.);
(xiv) The Paperwork Reduction Act of 1995 (44 U.S.C. § 3501 et seq.);
(xv) Federal Information Security Management Act of 2002 (44 U.S.C. § 3541 et seq.);
(xvi) The Communications Assistance for Law Enforcement Act (47 U.S.C. § 1001 et seq.);
(xvii) The Currency and Foreign Transactions Reporting Act of 1970, as amended (commonly known as the Bank Secrecy Act) (12 U.S.C. §§ 1829b and 1951-1959, 31 U.S.C. §§ 5311-5314 and 5316-5332), including the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, Title III of P.L. 107-56, as amended;
(xviii) Executive Order 12333, as amended, "United States Intelligence Activities, July 30, 2008," and any successor orders;
(xix) National Security Act of 1947 (50 U.S.C. § 3001 et seq.);
(xx) Foreign Intelligence Surveillance Act of 1978, as amended (50 U.S.C. § 1801 et seq.);
(xxi) The Civil Rights Act of 1964 (Pub.L. 88–352, 78 Stat. 241);
(xxii) The Americans with Disabilities Act (42 U.S.C. § 12101 et seq.);
(xxiii) The Fair Housing Act (42 U.S.C. § 3601 et seq.);
(xxiv) The Dodd-Frank Wall Street Reform and Consumer Protection Act (Pub. L. 111–203, 124 Stat. 1376–2223);
(xxv) The Equal Credit Opportunity Act (15 U.S.C. § 1691 et seq.);
(xxvi) The Age Discrimination in Employment Act (29 U.S.C. § 621 et seq.); and
(xxvii) The Genetic Information Nondiscrimination Act (Pub. L. 110–233, 122 Stat. 881).

(B) CHILDREN'S PRIVACY. -- Nothing in this Act may be construed to modify, limit, or supersede the operation of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. § 6501 et seq.), except for Section 5, subsection (5) of this Act.

(C) COMMUNICATIONS PRIVACY. -- If a covered entity is subject to a privacy or security requirement or provision of the Communications Act of 1934 (47 U.S.C. 151 et seq.), including but not limited to section 201, 222, or 631, or any regulations promulgated under that Act, such requirement, provision, or regulation shall have no force or effect, unless such requirement, provision, or regulation pertains to emergency services.