Public Knowledge

December 20, 2018

James Trilling, Bureau of Consumer Protection
Jah-Juin "Jared" Ho, Bureau of Consumer Protection
Daniel J. Gilman, Office of Policy Planning
Katherine Ambrogi, Office of Policy Planning
Constitution Center
Federal Trade Commission
400 7th Street, SW
Washington, DC 20024

Dear Mr. Trilling, Mr. Ho, Mr. Gilman, and Ms. Ambrogi,

On behalf of Public Knowledge, a public interest advocacy organization dedicated to promoting freedom of expression, an open internet, and access to affordable communications tools and creative works, we submit these comments in response to the Federal Trade Commission's Request for Public Comments Docket No. FTC-2018-0098: Hearings on Competition and Consumer Protection in 21st Century: Consumer Privacy, February 12-13, 2019.

It is no longer possible to participate in society without providing data to third parties that may, in and of themselves be personal, or that, when combined with other data and analyzed, may reveal intimate information. The consequences of this data acquisition, analysis, use, and sharing can be profound for individuals' lives. For example, online advertisers have used personal data to show certain job postings only to men[1] and to exclude African-Americans from seeing certain housing advertisements.[2] In the 2016 election, Russian agents used social networking data to target advertisements to African-Americans to urge them not to vote.[3] Data exploitation enables "unequal consumer treatment, financial fraud, identity theft, manipulative marketing, and discrimination."[4] Against this backdrop, the FTC's hearings on consumer privacy could not be timelier. These comments will proceed by addressing many of the FTC's specific questions in turn.

- **What are the actual and potential risks for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these risks?**

There are several ways information collection, sharing, aggregation, and use pose risk to both consumers and to competition. First, they may facilitate higher prices and reduce competition. In some homogeneous markets, vendors may be able to engage in tacit collusion through AI

[1] *See* UPTURN, LEVELING THE PLATFORM: REAL TRANSPARENCY FOR PAID MESSAGES ON FACEBOOK (May 2018).
[2] Julia Angwin, Ariana Tobin, and Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users By Race*, PROPUBLICA, Nov. 21, 2017.
[3] Natasha Singer, *Just Don't Call It Privacy*, NY TIMES, Sept. 23, 2018, https://www.nytimes.com/2018/09/22/sunday-review/privacy-hearing-amazon-google.html.
[4] *Id.*

systems.[5] Algorithms can monitor prices and other terms of sale,[6] giving companies a more detailed view of the market in nearly real-time,[7] allowing them to adjust to market changes more quickly and reliably,[8] and diminishing their need to cut prices to stay competitive.[9] Notably, this sort of behavior would not violate existing antitrust laws, because it does not involve an agreement to fix prices.

Moreover, pervasive data collection, sharing, aggregation, and use allow companies to develop detailed profiles of their customers' psychologies[10] and willingness to pay.[11] This enables "personalized pricing strategies"[12] with precise manipulations of consumer choices.[13] These insights into, and power over, customer behavior ultimately may help firms maximize profit to the net detriment of their customers.[14] Aside from their aggregate effects, supercharged price discrimination and other forms of hyper-targeted marketing could have disparate impacts on particularly vulnerable groups. These distributional possibilities alone warrant close examination.

The potential of artificial intelligence to limit consumer choice is even greater with digital assistants, like Amazon's Alexa, Google Home, Apple's HomePod, and Siri. If consumers switch from web-based searches to digital assistants, they may do less comparison shopping, as digital assistants increasingly respond to queries with a single response rather than a menu of options.[15] This is one example of a larger phenomenon that merits scrutiny: when algorithms determine what is "relevant" to a particular consumer, consumers are unaware of the options they never see.[16]

This informational filtering can be particularly harmful for marginalized communities – for example, when employers consciously use amassed data and algorithms to keep older workers

---

[5] *E.g.* A. Erachi & M.E. Stucke, Note, *Algorithmic Collusion: Problems and Counter-Measures*, 25 OECD ROUNDTABLE ON ALGORITHMS & COLLUSION, 1, 6 (2017).
[6] *Id*.
[7] Maurice E. Stucke & Ariel Ezrachi, *How Pricing Bots Could Form Cartels and Make Things More Expensive*, HARV. BUS. REV., Oct. 27, 2016, https://hbr.org/2016/10/how-pricing-bots-could-form-cartels-and-make-things-more-expensive.
[8] Michal S. Gal, *Algorithmic-Facilitated Coordination: Market and Legal Solutions*, CPI ANTITRUST CHRONICLE, May 2017, https://www.competitionpolicyinternational.com/wp-content/uploads/2017/05/CPI-Gal.pdf.
[9] A. Erachi & M.E. Stucke, Note, *Algorithmic Collusion: Problems and Counter-Measures*, 25 OECD ROUNDTABLE ON ALGORITHMS & COLLUSION, 1, 6 (2017).
[10] Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014).
[11] A. Erachi & M.E. Stucke, Note, *Algorithmic Collusion: Problems and Counter-Measures*, 25 OECD ROUNDTABLE ON ALGORITHMS & COLLUSION, 1, 12 (2017).
[12] *Id*.
[13] Michal Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 HARV. J. OF L. & TECH. 309, 324 (2017).
[14] Ramsi A. Woodcock, *The Power of the Bargaining Robot*, CPI ANTITRUST CHRONICLE, May 2017, https://www.competitionpolicyinternational.com/wp-content/uploads/2017/05/CPI-Woodcock.pdf; *see also* Michal S. Gal, *Algorithmic-Facilitated Coordination: Market and Legal Solutions*, CPI ANTITRUST CHRONICLE, May 2017, https://www.competitionpolicyinternational.com/wp-content/uploads/2017/05/CPI-Gal.pdf.
[15] *See* Maurice E. Stucke & Ariel Ezrachi, *How Digital Assistants Can Harm Our Economy, Privacy, and Democracy*, 32 BERKELEY TECH L.J. 1239, 1268 (2017).
[16] Michal Gal, *Algorithmic Challenges to Autonomous Choice*, at 3 (2017).

from seeing certain job postings,[17] or when landlords use data and algorithms to prevent racial minorities from seeing certain housing advertisements.[18] Even when humans are not intentionally aiming for such outcomes, the training data used to "teach" artificial intelligence often reflect entrenched historical biases, and artificial intelligence often magnifies those biases. For example, researchers at Carnegie Mellon and the International Computer Science Institute found that user "profiles . . . pegged as male were much more likely to be shown ads for higher-paying executive jobs than those . . . identified as female – even though the simulated users were otherwise equivalent."[19]

Discriminatory advertising not only occurs because of biased training data, but also because of flawed micro-auctions for internet advertising. For example, at the FTC's hearings on The Intersection of Big Data, Privacy, and Competition, Leigh Freund of the Network Advertising Initiative explained that women see fewer advertisements for job postings, because shopping advertisers outbid employers in the micro-auctions for female audiences.[20] While these auctions may seem "fair" by one metric – advertisements are sold to the highest bidder – they are unfair by other metrics, because they serve to systematically exclude women from seeing and therefore accessing opportunities.

- **The use of "big data" in automated decisionmaking has generated considerable discussion among privacy stakeholders. Do risks of information collection, sharing, aggregation, and use include risks related to potential biases in algorithms? Do they include risks related to use of information in risk scoring, differential pricing, and other individualized marketing practices? Should consideration of such risks depend on the accuracy of the underlying predictions? Do such risks differ when data is being collected and analyzed by a computer rather than a human?**

As algorithms are increasingly used to determine who sees a job posting or apartment listing, whose resume makes it through an initial screen, whether someone is offered a credit card, or what level of financial aid she receives,[21] the training data used in these systems becomes particularly important. Artificial intelligence is taught correlation, not causation. A training data set that features CEOs of Fortune 500 companies, for example, is likely to privilege male job applicants. A training data set that features historical home loan data is more likely to match Black and Latino borrowers to higher priced products, because historically, Blacks and Latinos have been

---

[17] Julia Angwin, Noam Scheiber, & Ariana Tobin, *Facebook Job Ads Raise Concerns About Age Discrimination*, NYTIMES, Dec. 20, 2017, https://www.nytimes.com/2017/12/20/business/facebook-job-ads.html.

[18] Julia Angwin, Ariana Tobin, & Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users By Race*, PROPUBLICA, Nov. 21, 2017, https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin.

[19] Sarah Wachter-Boettcher, *Why You Can't Trust AI to Make Unbiased Hiring Decisions*, TIME, Oct. 25, 2017, http://time.com/4993431/ai-recruiting-tools-do-not-eliminate-bias/.

[20] Leigh Freund, Testimony on Competition and Consumer Protection Issues in Online Advertising Before the Federal Trade Commission (Nov. 7, 2018).

[21] Saranya Vijayakumar, *Algorithmic Decision-Making*, HARV. POL. REV., June 28, 2017, http://harvardpolitics.com/covers/algorithmic-decision-making-to-what-extent-should-computers-make-decisions-for-society/; Will Knight, *Biased Algorithms Are Everywhere, and No One Seems to Care*, MIT TECH. REV., July 12, 2017, https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care/.

targeted for riskier financial products.[22] In fact, researchers at University of California Berkeley recently found that both human and online lenders profit by charging Black and Latinx borrowers substantially the same higher rates.[23]

But, bias is not the only risk posed by algorithms. For example, researchers at the Wall Street Journal discovered that Staples.com shows individuals who live near rival stores lower prices for staplers on its website.[24] Because stores are more likely to be situated in wealthier areas, this practice often means that Staples is charging poorer people higher prices.[25]

The FTC asks whether "consideration of such risks [should] depend on the accuracy of the underlying predictions." The FTC should consider what it means for an algorithm to be "accurate." As described above, algorithms are trained on correlation, not causation. To use the example of lending, "algorithms may take into account a borrower's neighborhood – noting who lives in banking deserts – or other characteristics such as their high school or college."[26] The algorithm may then "accurately" predict a higher percentage of people living in banking deserts default on loans. This prediction, even if correct in the aggregate, may or may not be "accurate" as to the particular borrower under consideration. And, if the particular borrower does default on his or her loan, is that because the algorithm was "accurate" in its prediction or because the algorithm assigned the borrower too high an interest rate, and had a more appropriate interest rate been assigned, the borrower would not have defaulted? In short, accuracy in the context of predictive analytics may be indeterminate. And, moreover, when automated decisionmaking entrenches systematic biases, the harms and risks are particularly acute, regardless of the system's accuracy as to particular individuals.

Absent conscious intervention, automated decisionmaking is likely to discriminate against the same groups of people who have traditionally been discriminated against – racial and religious minorities, lesbian, gay, bisexual, and transgender people, women, low income households, and those with disabilities. The risks are different – or perhaps more greatly magnified – than when data are collected and analyzed by a human, because many people assume that machines are immune from bias. The use of automated decisionmaking is likely to obscure biases, making them harder to confront and more dangerous to society and to consumer welfare.[27] In addition, "big data" and automated decisionmaking permit the proliferation of harm at a scale that would simply be impossible when data are collected and analyzed by humans.

---

[22] Gillian B. White, *Why Blacks and Hispanics Have Such Expensive Mortgages*, THE ATLANTIC, Feb. 25, 2016, https://www.theatlantic.com/business/archive/2016/02/blacks-hispanics-mortgages/471024/.

[23] Tracy Jan, *Are you a minority borrower? You might want to think twice about using an online lender*, WASH. POST, Nov. 14, 2018, https://www.washingtonpost.com/business/2018/11/14/are-you-minority-borrower-you-might-want-think-twice-about-using-an-online-lender/.

[24] Jennifer Valentino-DeVries, Jeremy Singer-Vine, & Ashkan Soltani, *Websites Vary Prices, Deals Based on Users' Information*, WALL STREET J., Dec. 24, 2012, https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

[25] *Id.*

[26] Tracy Jan, *Are you a minority borrower? You might want to think twice about using an online lender*, WASH. POST, Nov. 14, 2018, https://www.washingtonpost.com/business/2018/11/14/are-you-minority-borrower-you-might-want-think-twice-about-using-an-online-lender/.

[27] Will Knight, *Biased Algorithms Are Everywhere, and No One Seems to Care*, MIT TECH. REV., July 12, 2017, https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care/.

For these reasons, in addition to considering how to regulate and oversee training data, the Federal Trade Commission should consider when and how it may be necessary to encourage and/or require transparency for the algorithms themselves, to lift the veil on opaque decision-making processes and enable consumers to better understand how algorithmic decisions are made and what predictive analytics say about them.[28]

- **Should privacy protections depend on the sensitivity of data?**

No, privacy protections should not depend on the sensitivity of the data. The so-called sensitive/non-sensitive distinction, which provides heightened protections to so-called sensitive information, like first and last name, social security numbers, bank account numbers, etc., and lesser protections to other information is increasingly illogical in today's world and should be eschewed. So-called non-sensitive information can be aggregated to reveal sensitive information, and, in fact, some non-sensitive information, in isolation, may reveal sensitive information. For example, while one's health status is frequently considered sensitive, one's shopping history is not. If one is shopping at TLC Direct[29] and Headcovers Unlimited,[30] two websites that specialize in hats for chemotherapy patients, it may be trivial to infer her health status.

Furthermore, so-called non-sensitive information can be used for purposes that are quite sensitive. For example, if Cambridge Analytica (and, for that matter, the Obama campaign)[31] is to be believed, so-called non-sensitive information such as social media likes can be used for highly sensitive activities such as influencing individuals in the voting booth. In addition, sensitivity is highly subjective. Different individuals are likely to perceive different data points' sensitivity levels differently.

For these reasons, any line drawing around the sensitivity of information is inherently arbitrary. Thus, any federal privacy regime must provide robust protections for all personal information – that is, any information that is reasonably linkable, directly or indirectly, to a specific consumer, household, or device[32] – and not merely for so-called sensitive information. Eschewing the sensitive/non-sensitive distinction is critical for ensuring that any federal privacy legislation stands the test of time.

- **Should privacy protection depend on, or allow for, consumer variation in privacy preferences? Why or why not? What are the appropriate tradeoffs to consider? If desired, how should this flexibility be implemented?**

Through meaningful consumer choice, there should be some space for variations in consumer privacy protections based on variations in consumer preferences. Until the digital age,

---

[28] *See Algorithmic Transparency: End Secret Profiling*, EPIC, https://epic.org/algorithmic-transparency/ (last accessed Aug. 13, 2018).
[29] TLC DIRECT, https://www.tlcdirect.org (last visited Nov. 2, 2018).
[30] HEADCOVERS UNLIMITED, https://www.headcovers.com (last visited Nov. 2, 2018).
[31] Tim Murphy, *Inside the Obama Campaign's Hard Drive*, MOTHER JONES, Sept./Oct. 2012, https://www.motherjones.com/politics/2012/10/harper-reed-obama-campaign-microtargeting/.
[32] *E.g.* CAL. CIV. CODE § 1798.135(o)(1).

individual ownership and control of one's own personal information was the basis for privacy law in the United States.[33] Adhering to this principle, meaningful opportunities for consumer control and consent are important pieces of any privacy regime. Consumers must have meaningful opportunities to freely and affirmatively consent to data collection, retention, and sharing. And, that consent should be as granular as possible. For example, a user should be able to consent for her data to be used for research purposes, but not for targeted advertising – or vice-versa. Consent must be real rather than implied in the fine print of a terms of service or coerced as a condition of service or through manipulative design choices. Consumers must also have the ability to withdraw their consent if they no longer wish for a company to use and retain their personal data. In addition, service should not be contingent on the sharing of data that are not necessary to render the service.[34]

However, any privacy regime cannot rely exclusively on consumer choice. Research demonstrates that individuals have difficulty imagining future harms that may come from data sharing and use, particularly when faced with the need or desire for access to a particular product or service in the present. This makes it difficult for individuals to make "informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal information."[35] For this reason, some additional consumer protections must be layered on top of notice and consent, and it is likely that some collection and uses of data should be foreclosed outright.

- **Should the Commission's privacy enforcement and policy work be limited to market-based harms? Why or why not?**

No, the FTC's privacy enforcement and policy work should not be limited to market-based harms. This approach would be a one-eighty from the traditional approach to privacy in the U.S. Since the days of Justice Brandeis, individual ownership[36] and control of one's own personal information has been the basis for U.S. privacy law.[37] With this principle in mind, privacy is a fundamental right, and the harm occurs when personal information is acquired, accessed, or used in a way that is unanticipated or unauthorized by the individual to whom the information pertains, regardless of the concomitant risks.

Moreover, if the FTC is to focus solely on market-based harms, it must define them to include more than straightforward financial injury. Financial injury is a very small subset of the

---

[33] HAROLD FELD, PRINCIPLES FOR PRIVACY LEGISLATION: PUTTING PEOPLE BACK IN CONTROL OF THEIR INFORMATION 19 – 20 (Public Knowledge, 2017).

[34] While it may be appropriate for a non-essential service like Facebook to charge users a fee in lieu of selling their data, *see* Alex Johnson and Erik Ortiz, *Without data-targeted ads, Facebook would look like a pay service, Sandberg says*, NBC NEWS, Apr. 5, 2018, https://www.nbcnews.com/tech/social-media/users-would-have-pay-opt-out-all-facebook-ads-sheryl-n863151, such an approach is unacceptable for services that are integral for participation in society. Individuals should be able to access health care, education, housing, and other essential services without compromising their personal information or having to pay extra for their fundamental right to privacy.

[35] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1881 (2013).

[36] When we use "ownership," we do not necessarily imply a formal, alienable property right, but rather a philosophical framework.

[37] HAROLD FELD, PRINCIPLES FOR PRIVACY LEGISLATION: PUTTING PEOPLE BACK IN CONTROL OF THEIR INFORMATION 19 – 20 (Public Knowledge, 2017).

harms that can arise from misuse of data or data breach, and it is among the hardest harms to prove. Even where financial loss arises from a data breach or the misuse of data – say, where a credit card number is stolen and fraudulent purchases are made – it is difficult to trace that stolen credit card to one particular data breach.[38] And, where it is possible to trace back to the particular data breach, banks often reimburse customers for fraudulent purchases, obviating any actual financial loss.[39]

In addition to financial harm, a data breach may expose information that could be embarrassing or cause reputational harm, undermining one's employment or social prospects. Irresponsible data use can enable unfair price discrimination, limit awareness of opportunities, and contribute to employment, housing, health care, and other forms of discrimination. These are arguably market-based harms, although in many cases they may be hard to quantify.

Moreover, many of the most pernicious harms associated with data breach and misuse of data are likely not market-based harms. For example, data that fall into the wrong hands could re-endanger a domestic violence victim. Harms may also come in the form of Cambridge Analytica-style "psychographics," misinformation, distortions of the public record, or undermining public trust in U.S. democratic institutions. Irresponsible data use can also exacerbate informational disparities. And, the risks associated with data use and abuse may change as technology changes.

This is not to suggest that a privacy regime must solve for all of society's ills, but it is to say that in order to sufficiently protect consumers in the digital age, the FTC must take into account the full panoply of harms – including those that may arise in the future – whether or not they are market-based.

- **In general, privacy interventions could be implemented at many different points in the process of collecting, processing, and using data. For example, certain collections could be banned, certain uses could be opt-in only, or certain types of processing could trigger disclosure requirements. Where should interventions be focused? What interventions are appropriate?**

Because abuse and misuse can happen at all stages, it is imperative that any privacy regime cover the full lifecycle of data, including collection, processing, using, retaining, and sharing data. Appropriate interventions include the following:

1. *Meaningful Notice and Consent*

Until the digital age, individual ownership and control of one's own personal information was the basis for privacy law in the United States.[40] We should return to this principle. While we cannot avoid sharing information with some third parties, we can have greater control over that information. At a minimum, consumers should have a right to know a) what information is being

---

[38] *See* Nicole Hong, *For Consumers, Injury Is Hard to Prove in Data-Breach Cases*, WALL STREET J., June 26, 2016, https://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988.
[39] *Id.*
[40] HAROLD FELD, PRINCIPLES FOR PRIVACY LEGISLATION: PUTTING PEOPLE BACK IN CONTROL OF THEIR INFORMATION 19 – 20 (Public Knowledge, 2017).

collected and retained about them; b) how long that information is being retained; c) for what purposes that information is being retained; d) whether the retained information is identifiable, pseudo-anonymized, or anonymized; e) whether and how that information is being used; f) with whom that information is being shared; g) for what purposes that information is being shared; h) under what rubric that information is being shared (for free, in exchange for compensation, subject to a probable cause warrant, etc.); and (i) whether such information is being protected with industry-recognized best security practices.[41]

It is imperative that this notice be meaningful and effective, which means that it cannot be buried in the fine print of a lengthy privacy policy or terms of service agreement. Consumers and companies know that consumers do not typically read privacy policies or terms of service agreements. Indeed, researchers at Carnegie Mellon estimate that it would take seventy-six work days for an individual to read all of the privacy policies she encounters in a year.[42] Companies take advantage of this common knowledge to bury provisions that they know consumers are unlikely to agree to in the fine print of these agreements.

Moreover, notice alone is insufficient. Consumers must also have meaningful opportunities to freely and affirmatively consent to data collection, retention, use, and sharing. And, that consent should be as granular as possible. For example, a user should be able to consent for her data to be used for research purposes, but not for targeted advertising – or vice-versa. As with notice, the consent must be real rather than implied in the fine print of a terms of service. Consumers must also have the ability to withdraw their consent if they no longer wish for a company to use and retain their personal data, and they should be able to port their data in a machine-readable format to another service, if they so desire.[43] In addition, service should not be contingent on the sharing of data that are not necessary to render the service.[44]

---

[41] Consumer advocates are not alone in calling for meaningful notice. Both the Internet Association and The Software Alliance also call for notice. INTERNET ASSOCIATION, IA PRIVACY PRINCIPLES FOR A MODERN NATIONAL REGULATORY FRAMEWORK (2018) ("Transparency. Individuals should have the ability to know if and how personal information they provide is used and shared, who it's being shared with, and why it's being shared."); THE SOFTWARE ALLIANCE, BSA PRIVACY PRINCIPLES (2018) ("Transparency[.] Organizations should provide clear and accessible explanations of their practices for handling personal data, including the categories of personal data they collect, the type of third parties with whom they share data, and the description of processes the organization maintains to review, request changes to, request a copy of, or delete personal data.")

[42] Alexis C. Madrigal, *Reading the Privacy Policies you Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC, Mar. 1, 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[43] This is another recommendation where advocates and industry align. *See* THE SOFTWARE ALLIANCE, BSA PRIVACY PRINCIPLES (2018).

[44] While it may be appropriate for a non-essential service like Facebook to charge users a fee in lieu of selling their data, *see* Alex Johnson and Erik Ortiz, *Without data-targeted ads, Facebook would look like a pay service, Sandberg says*, NBC NEWS, Apr. 5, 2018, https://www.nbcnews.com/tech/social-media/users-would-have-pay-opt-out-all-facebook-ads-sheryl-n863151, such an approach is unacceptable for services that are integral for participation in society. Individuals should be able to access health care, education, housing, and other essential services without compromising their personal information or having to pay extra for their fundamental right to privacy.

2. Robust Security Requirements

Entities that are stewards of our personal information should be expected to adhere to recognized best practices to secure the information. This is particularly true when an individual cannot avoid sharing the information without foregoing critical services or declining to participate in modern society.

Relatedly, entities should be required to adhere to privacy-by-design and by default.[45] Entities should be encouraged to employ encryption and pseudo-anonymization or de-identification to protect consumers' private information,[46] and security mechanisms should be regularly evaluated. Importantly, these evaluations must be publicly reported to enable transparency and accountability. In addition, the government should act as convener of any multi-stakeholder process to develop privacy and/or security standards. Facebook/Cambridge Analytica, as well as the cascade of recent data breaches, has demonstrated that industry cannot be trusted to police itself.

Furthermore, entities that experience a data breach should be required to notify consumers of the breach as soon as practicable after it occurs without any required showing of "harm." Given the philosophical consensus that individuals own their own data,[47] the harm occurs when personal information is acquired or accessed in a way that is unanticipated or unauthorized by the individual to whom the information pertains.[48] Notifying consumers as soon as practicable after a breach will also allow individuals to take prophylactic measures to protect themselves from further injury. Moreover, entrenching the harm standard would simply allow the entity that has already failed to sufficiently protect sensitive personal information to determine, in its sole discretion – when it has every financial incentive to keep a data breach secret – whether or not consumers have been or will be harmed and thus whether or not consumers should be informed of the breach.

3. Data Minimization

Data minimization is an important security measure; data that are not collected or retained are also not targets for data thieves and other malicious actors. Moreover, data minimization can help prevent some of the harms that arise from misuse of data, like unfair price discrimination, limiting awareness of opportunities, and perpetuating employment, housing, health care, and other forms of discrimination – all risks that multiply when entities are able to build increasingly detailed consumer profiles.

---

[45] Again here there are synergies with industry recommendations. *See id.*; U.S. CHAMBER, PRIVACY PRINCIPLES (2018).

[46] It is trivial to re-identify de-identified or pseudo-anonymized data. *See generally* Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 GEO. L. TECH. REV. 202 (2017). Therefore, any federal policy must require that entities employ technical and policy measures to ensure that the personal data are not re-identified.

[47] When we use "ownership," we do not necessarily imply a formal, alienable property right, but rather a philosophical framework. *See* pp. 2, 5 *supra*.

[48] Additionally, traditional economic or dignitary harms may be present in fact, but difficult or impossible to demonstrate or quantify, especially for an individual.

At the same time, many of the data uses that are sometimes claimed to require widespread information collection, such as machine learning, in fact do not always require such copious collection, as techniques such as differential privacy[49] and federated learning[50] demonstrate.

For these reasons, the presumption should be that only data necessary for the requested transaction will be collected and retained, absent explicit consumer consent.

4. Privacy-by-Design and by Default

Entities that collect, maintain, use, store, and/or share individuals' personal information should be required to adhere to privacy-by-design and by default.[51] Too often the default is destiny; most people never change default settings.[52] Personal information is just that – personal. Setting the defaults to the most privacy-enhancing option best positions individuals to decide what is done with their data and with whom their data are shared.

5. Data Portability and Interoperability

Individuals should be able to port their data in a machine-readable format to another service, if they so desire.[53] Data portability is competition-enhancing and may be privacy-enhancing, if new entrants elect to compete based on privacy protections.

However, there are some tricky questions that must be resolved to mitigate privacy risks from portability. For example, if an individual's friend uploads a picture of that individual to a social network, can that individual port the picture and its metadata? Can the friend? If two people are connected only on a social network, can one export the other's contact information? What kind of consent is required, if any, from the second individual?

Moreover, for data portability to be widely useful in practice, some level of interoperability will usually be necessary. Incumbent platforms, particularly incumbent social networks, benefit from network effects: individuals want to be on the sites that their friends are on. Unless individuals are able to communicate across platforms, a vanishingly small number of platforms will continue to dominate as people congregate to the sites where their friends are.

6. Access and Correction

Individuals should be able to access both the data they have provided to entities and the inferences those entities have made about them based on their data. Inferences are particularly

---

[49] *Differential Privacy Overview*, APPLE, https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf (last visited Nov. 8, 2018).

[50] Brendan McMahan and Daniel Ramage, Google AI Blog, *Federated Learning: Collaborative Machine Learning without Centralized Training Data* (Apr. 6, 2017) (last visited Nov. 8, 2018).

[51] Here there are synergies with industry recommendations. *See id.*; U.S. CHAMBER, PRIVACY PRINCIPLES (2018).

[52] Lena V. Groeger, *Set It and Forget It: How Default Settings Rule the World*, PROPUBLICA, July 27, 2016, https://www.propublica.org/article/set-it-and-forget-it-how-default-settings-rule-the-world.

[53] This is another recommendation where advocates and industry align. *See* THE SOFTWARE ALLIANCE, BSA PRIVACY PRINCIPLES (2018).

likely to facilitate some of the harms we are concerned about, like unfair price discrimination, limiting awareness of opportunities, and perpetuating employment, housing, health care, and other forms of discrimination. Only by knowing about these inferences can individuals even attempt to guard against these harms.

Individuals should also have a qualified right to "rectify, complete, amend, or delete"[54] data. Policymakers should ensure that individuals cannot "rectify" or "amend" data if the corrections they seek are inaccurate or would distort the public record. Nor should individuals be permitted to delete data where data deletion would violate others' First Amendment rights to receive information. However, individuals should generally have the opportunity to rectify, amend, or delete data, as well as the opportunity to understand why the entities that maintain data about them make the decisions they do and the opportunity to challenge those decisions, with a fair process, where they disagree.[55]

7. Additional Protections

A notice and consent regime by itself is insufficient to protect consumers in the digital age. There is an information and power asymmetry between entities that collect data and individual consumers that makes it difficult for all but the savviest consumers to protect their personal information from misuse and abuse. Consequently, policymakers should step in to ensure that data cannot be used to unfairly discriminate against already marginalized populations. This may also be achieved by perusing transparency and accountability in automated decision-making, particularly when it concerns essential services and opportunities, like housing, jobs, health care, education, and lending. If regulators, watchdog organizations, and, indeed, individuals are better able to understand algorithmic decision-making, they may be better positioned to mitigate and guard against some of the more pernicious risks associated with big data.[56] In addition, it may be desirable to layer use restrictions, collection restrictions, sharing restrictions, and anti-discrimination protections on top of any notice and consent regime.

- **How can firms that interface directly with consumers foster accountability of third parties to whom they transfer consumer data?**

Entities that interface directly with consumers must foster accountability of third parties to whom they transfer consumer data. Accountability mechanisms should include contractual provisions promising that third parties will adhere to the privacy requirements imposed upon and promises made by the consumer-facing entity and laying out which party is responsible for notifying consumers and making consumers whole in the event of a data breach or misuse or unauthorized use of data, as well as auditing requirements to ensure that the contractual provisions are adhered to.

---

[54] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48602 (Sept. 26, 2018).
[55] For a much more detailed discussion, *see* JOHN BERGMAYER, EVEN UNDER KIND MASTERS: A PROPOSAL TO REQUIRE THAT DOMINANT PLATFORMS ACCORD THEIR USERS DUE PROCESS (Public Knowledge, 2018).
[56] *See generally* PUBLIC INTEREST PRIVACY PRINCIPLES (2018) (included as Appendix C).

- **What are the effects, if any, on competition and innovation from privacy interventions, including from policies such as data minimization, privacy by design, and other principles that the Commission has recommended?**

To an extent, privacy interventions may require entities to invest more in privacy, which may mean they have less to spend on other things. Some maintain that privacy interventions can also favor existing large firms that can more easily comply by retrofitting their operations than existing small firms can. However, concerns that privacy-by-design, data minimization, and other privacy protections will stifle innovation and competition are likely over-blown. Innovation can take place in a privacy-preserving context, and the desire to protect privacy while continuing to offer particular kinds of services can spur new forms of innovation. New entrants are accustomed to accounting for and accommodating laws and regulations, and can have an advantage over incumbents with legacy operations. As Dr. Andrea Jelinek, chair of the European Data Protection Board, testified before the Senate Commerce Committee, new entrants into the market in Europe simply take the General Data Protection Regulation (GDPR) into account and employ privacy-by-design and by default into their products from the beginning; Europe has not seen a decline in innovation since GDPR implementation.[57]

Nor should we encourage market entry at any cost. For example, while there is insufficient competition in the pharmaceutical industry, as a society, the United States has decided not to permit unsavory characters to sell snake oil on the sidewalk. Such salespeople might increase competition in the pharmaceutical industry and might reduce prices, but would do so at the expense of public welfare. Similarly, irresponsible companies should not have free rein to misuse, abuse, and fail to safeguard consumers' data in the name of competition and innovation. Indeed, such entities may even crowd out more consumer-friendly alternatives.

- **If businesses offer consumers choices with respect to privacy protections, can consumers be provided the right balance of information, i.e., enough to inform the choice, but not so much that it overwhelms the decisionmaker? What is the best way to strike that balance?**

As described above, consumers and entities know that consumers do not typically read privacy policies or terms of service agreements. Indeed, it would be both irrational and inefficient for consumers to read privacy policies; researchers at Carnegie Mellon estimate that it would take seventy-six work days for an individual to read all of the privacy policies she encounters in a year.[58] Entities take advantage of this common knowledge to bury provisions that they know consumers are unlikely to agree to in the fine print of these agreements. Privacy notices must be done more effectively. The FTC should explore "nutrition label"-style approaches to privacy policies where salient information for consumers could be conveyed, in plain language, on a single

---

[57] *Consumer Data Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act: Hearing Before the S. Comm. on Commerce, Science, & Transportation*, 115th Cong. (2018) (statement of Andrea Jelinek, Chair, European Data Protection Board).

[58] Alexis C. Madrigal, *Reading the Privacy Policies you Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC, Mar. 1, 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

cellphone screen. In general, consumer-facing privacy policies should be concise, intelligible, clear, and prominent; they should use plain language and visualizations where appropriate.[59]

It may be appropriate for any federal privacy regime to additionally mandate a separate, legal disclosure that contains the breadth of information included in today's privacy policies and terms of service and that may, indeed, be more detailed than today's policies. The purpose of this disclosure would be a legal one – to permit the relevant administrative agency, as well as watchdog groups, to better understand entities' data practices and hold entities accountable when they fail to live up to their promises or when their promises fail to adhere to the law or to consumer expectations.

The relevant agency, most likely the FTC, should be imbued with APA rulemaking authority to develop the details of any notice regime.

- **Some academic studies have highlighted differences between consumers' stated preferences on privacy and their "revealed" preferences, as demonstrated by specific behaviors. What are the explanations for the differences?**

Some academics have interpreted data about particular online behaviors, such as continuing to use Facebook or declining to opt-out of targeted advertising as indicating that consumers do not necessarily care about privacy, even when consumers repeatedly articulate their desire for privacy. There are, however, other explanations for these consumer behaviors.

For example, consumers may feel obligated to use Facebook to communicate with loved ones or Twitter for work purposes. In too many contexts, the choice is to sacrifice privacy or to decline to participate in modern society. That is not a viable option for most people. This conclusion comports with the results of an Annenberg School study, which found that

> a majority of Americans are resigned to giving up their data—and that is why many appear to be engaging in tradeoffs. Resignation occurs when a person believes an undesirable outcome is inevitable and feels powerless to stop it. Rather than feeling able to make choices, Americans believe it is futile to manage what companies can learn about them. Our study reveals that more than half do not want to lose control over their information but also believe this loss of control has already happened.[60]

Additionally, 92% of Facebook users do change the social network's default privacy settings.[61] This strongly suggests that consumers wish to preserve their privacy by choosing which audiences they share information with – and, indeed, they believe that they are limiting the audiences for their posts.

---

[59] *See* Information Transparency & Personal Data Control Act, H.R. 6864, 115th Cong. § 2(a)(2) (2018).
[60] Joseph Turow, Michael Hennessy, & Nora Draper, *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers And Opening Them Up To Exploitation* (Annenberg School for Comm., U. of Penn.), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.
[61] Emil Protalinksi, *13 million US Facebook users don't change privacy settings*, ZDNet, May 3, 2012, https://www.zdnet.com/article/13-million-us-facebook-users-dont-change-privacy-settings/.

Moreover, the advertising industry has, deliberately, it seems, made it unnecessarily difficult to understand – much less opt-out of – targeted advertising. The Future of Privacy Forum investigated which icon and associated phrase were most likely to convey to consumers that clicking on the icon/phrase would lead to disclosure information and options about behavioral advertising.[62] The Future of Privacy Forum found that the "asterisk man" icon and the phrases "Why did I get this ad?" and "Interest based ads" performed best. The phrase "Adchoice" performed noticeably less well.[63] The ad industry selected, instead of "asterisk man," a small "forward I" icon and the phrase AdChoices.[64] This can only be interpreted as a cynical attempt to hide pertinent information from consumers. Given that the advertising industry has made it difficult and confusing for individuals to opt-out of targeted advertising, it is disingenuous to suggest that the paucity of opt-outs means people do not care about privacy. It is more likely that they cannot figure out how to navigate a deliberately difficult system.

- **Given the evolution of technology, is the definition of de-identified data from the FTC's 2012 Privacy Report workable?**

The definition of de-identified data from the FTC's 2012 Privacy Report is workable, and all three portions of the definition – technical measures to de-identify the data, public commitments and internal policies not to reidentify the data, and contractual commitments from any third parties with whom data are shared not to re-identify the data – are extremely important. Technologically, it is trivial to reidentify deidentified data.[65] Therefore, any federal policy must require that entities employ technical and policy measures to ensure that the personal data are not reidentified. Moreover, federal policy should prioritize differential privacy and data minimization, techniques that obviate reidentification, particularly when the risk of reidentification is high.

- **What are existing and emerging legal frameworks for privacy protection? What are the benefits and drawbacks of each framework?**

In Europe and countries, such as Brazil that are adopting GDPR-like models,[66] privacy is a fundamental human right. While portions of GDPR would be culturally or even legally inappropriate and/or unworkable in the United States,[67] the idea of privacy as a fundamental human right is consistent with the traditional U.S. approach to privacy.[68] Public Knowledge has

---

[62] *See* FPF Staff, *Online Behavioral Advertising "Icon" Study*, FUTURE OF PRIVACY FORUM (Feb. 15 2010), https://fpf.org/2010/02/15/online-behavioral-advertising-icon-study/.

[63] *See id*.

[64] *See* Jonathan Mayer, *Tracking the Trackers: The AdChoices Icon*, STANFORD LAW SCHOOL: THE CENTER FOR INTERNET & SOCIETY (Aug. 18, 2011), http://cyberlaw.stanford.edu/blog/2011/08/tracking-trackers-adchoices-icon.

[65] *See generally* Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 GEO. L. TECH. REV. 202 (2017).

[66] Melanie Ramey, *Brazil's New General Data Privacy Law Follows GDPR Provisions*, INSIDE PRIVACY, COVINGTON & BURLING LLP, Aug. 20, 2018, https://www.insideprivacy.com/international/brazils-new-general-data-privacy-law-follows-gdpr-provisions/; Graham Greenleaf, *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*, 145 PRIVACY L. & BUS. INT'L REP. 10, 10 – 13 (2017).

[67] *See generally* Gus Rossi, *Is the GDPR Right for the United States?*, PUBLIC KNOWLEDGE, Apr. 9, 2018, https://www.publicknowledge.org/news-blog/blogs/is-the-gdpr-right-for-the-united-states.

[68] HAROLD FELD, PRINCIPLES FOR PRIVACY LEGISLATION: PUTTING PEOPLE BACK IN CONTROL OF THEIR INFORMATION 19 – 20 (Public Knowledge, 2017).

written at length about the benefits and drawbacks of the GDPR's approach, and that document is included as Appendix A.[69]

In contrast to GDPR, California's recently adopted privacy law maintains that the sale of consumer data and data breach are the only practices with which consumers and regulators should be concerned. Public Knowledge has also written at length about the benefits and drawbacks of California's approach, and that document is included as Appendix B.[70]

- **What are the tradeoffs between ex ante regulatory and ex post enforcement approaches to privacy protection?**

As the Commission well knows, the FTC, at present, only has the authority to respond to a privacy violation after it has occurred – in fact, the FTC is only able to impose penalties after a privacy violation has happened, the errant company has entered into a consent decree with the FTC and violated the consent decree, and the FTC has gone to court to sue the errant company. Furthermore, because resources are necessarily limited, the FTC is likely to only intervene in the most egregious cases. This *ex post* enforcement incentivizes smaller and less high-profile companies to engage in riskier privacy behavior, figuring they are unlikely to be the target of an FTC investigation given the Commission's scarce resources. This rubric is insufficient to protect consumer privacy in the digital age. Rather, the FTC should be in the business of preventing privacy harms before they happen – in addition to remedying privacy harms.

The Commission needs rulemaking authority to create *ex ante* rules of the road that provide predictability for companies and sufficient privacy protections for consumers.[71] Far from being a burden on the dynamic digital ecosystem, *ex ante* regulation provides certainty to companies that currently must rely on interpreting vague agency guidance and past enforcement actions and provides the FTC with the flexibility to adapt the rules to address market developments.

- **The U.S. has a number of privacy laws that cover conduct by certain entities that collect certain types of information, such as information about consumers' finances or health. Various statutes address personal health data, financial information, children's information, contents of communications, drivers' license data, video viewing data, genetic data, education data, data collected by government agencies, customer proprietary network information, and information collected and used to make certain decisions about consumers. Are there gaps that need to be filled for certain kinds of entities, data, or conduct? Why or why not?**

Sectoral privacy laws form the foundation of the U.S. privacy regime, and any comprehensive privacy regime should build upon rather than upend these laws. However, a comprehensive privacy law is necessary to protect the types of information not covered by these

---

[69] Gus Rossi, *Is the GDPR Right for the United States?,* PUBLIC KNOWLEDGE, Apr. 9, 2018, https://www.publicknowledge.org/news-blog/blogs/is-the-gdpr-right-for-the-united-states (included as Appendix A).
[70] Allie Bohm, *Is California's New Privacy Law Right for the United States?,* PUBLIC KNOWLEDGE, July 16, 2018, https://www.publicknowledge.org/news-blog/blogs/is-californias-new-privacy-law-right-for-the-united-states (included as Appendix B).
[71] *See id.*

laws. Indeed, advances in computing technology and the falling cost of data storage has permitted the acquisition, mining, use, storage, and sharing of data at a scale that was unimaginable even a decade ago, and it has made seemingly innocuous data points valuable for any number of uses. For example, Fitbit data are not considered health information covered by HIPAA even though they can reveal or indicate health information. It is not clear that the Facebook information that Cambridge Analytica purports was useful for "psychographics"[72] would be covered by any existing sectoral privacy law. Most metadata are not covered by existing sectoral privacy laws, even though they can be as intimate as the contents of communications.[73] Since Congress repealed the Federal Communications Commission's broadband privacy rule, ISPs have been free to do whatever they please with consumer data. The advertising industry's use of data is basically unregulated. This is not to suggest that the U.S. needs more sectoral privacy laws, but rather that the time is ripe for comprehensive privacy legislation.

- **Other than explicit statutory exemptions, are there limitations to the FTC's authority to protect consumers' privacy? If so, should they be removed? Why or why not? Should more limitations be implemented? Why or why not?**

The FTC's authority to protect consumers is limited both by the Commission's lack of resources and by its lack of rulemaking authority. Both of these impediments should be removed. Former FTC Commissioners and staff have lamented that the FTC is not sufficiently resourced to protect consumer privacy in the digital age.[74] Since 2010, FTC funding has fallen five percent.[75] The Commission is unable pay the competitive salaries necessary to lure technologists from the private sector and as a result suffers from a dearth of technical expertise.[76] If the FTC is to be a sufficient cop on the beat protecting consumer privacy, it simply must have the resources and technical expertise commensurate with the task.[77]

Furthermore, as described above, the FTC only has the authority to respond to a privacy violation after it has occurred and needs rulemaking authority in order to sufficiently protect consumers in the digital age. Rulemaking authority is particularly important because of the pace at

---

[72] *See generally* Allie Bohm, *Here's How Congress Should Respond to Facebook/Cambridge Analytica*, PUBLIC KNOWLEDGE, Mar. 23, 2018, https://www.publicknowledge.org/news-blog/blogs/heres-how-congress-should-respond-to-facebook-cambridge-analytica.

[73] Matthew Harwood, *My Life in Circles: Why Metadata is Incredibly Intimate*, ACLU FREE FUTURE, July 29, 2013, https://www.aclu.org/blog/national-security/secrecy/my-life-circles-why-metadata-incredibly-intimate.

[74] *E.g.* Terrell McSweeny, Former FTC Commissioner, Open Tech. Inst., Facebook After Cambridge Analytica: What Should We Do Now? (Apr. 5, 2018); Tony Romm, *The agency in charge of policing Facebook and Google is 103 years old. Can it modernize?*, WASH. POST, May 4, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/.

[75] David McCabe, *Mergers are spiking, but antitrust cop funding isn't*, AXIOS, May 7, 2018, https://www.axios.com/antitrust-doj-ftc-funding-2f69ed8c-b486-4a08-ab57-d3535ae43b52.html.

[76] Tony Romm, *The agency in charge of policing Facebook and Google is 103 years old. Can it modernize?*, WASH. POST, May 4, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/; *see also* Terrell McSweeny, Former FTC Commissioner, Open Tech. Inst., Facebook After Cambridge Analytica: What Should We Do Now? (Apr. 5, 2018).

[77] *See* Dylan Gilbert, *The FTC Must Be Empowered to Protect Our Privacy*, PUBLIC KNOWLEDGE, June 18, 2018, https://www.publicknowledge.org/news-blog/blogs/the-ftc-must-be-empowered-to-protect-our-privacy.

which Congress legislates. The legislative process is, in fact, designed to be slow.[78] The Telecommunications Act was last updated in 1996.[79] The Electronic Communications Privacy Act was authored in 1986 – before the advent of the World Wide Web – and has not meaningfully been updated since.[80] Google is currently rolling out an update to Gmail.[81] Apple released its latest operating system for its iPhones and iPads on September 17, 2018.[82] Congress cannot hope to keep pace with the rate at which the technology industry innovates. Therefore, it is incumbent upon Congress to empower an oversight agency, which can move more nimbly than Congress can, with rulemaking authority so that the agency can update the rules to keep up with technological changes, as well as with new harms that may arise as technology develops.

However, the FTC should not supplant the FCC's authority over ISPs and communications networks, its traditional areas of expertise and jurisdiction. Rather, any comprehensive privacy regime should build on the FCC and the FTC's respective years of experience with and knowledge of the entities they oversee and should preserve FCC authority.

- **If the U.S. were to enact federal privacy legislation, what should such legislation look like?**

The U.S. should enact comprehensive privacy legislation. It is widely agreed that any comprehensive privacy legislation must cover both ISPs and edge providers.[83] However, comprehensive legislation must recognize the disparate ways that different entities use, collect, and, indeed, require personal data, and it must treat different entities differently. For example, an ISP requires an individual's physical address in order to deliver internet service; Facebook or Twitter does not need an individual's physical address in order for their service to function. Similarly, by virtue of owning the pipes, ISPs are able to collect significantly more data about individuals than edge providers can; ISPs can view the entirety of an individual's internet browsing activity; they also have information about whether the individual pays his or her cable bill on time. A typical edge provider – even one that makes prolific use of tracking pixels on third party websites – may have only a fraction of an ISP's insights on a given consumer. This means that if legislation allows for exceptions for data used for legitimate business purposes, it is appropriate to tailor what data are exempted for different entities (rather than, say, exempting all address information, because ISPs need it). All entities in the ecosystem should, of course, have the same obligations to protect and adhere to notice and consent and other requirements for the data they do collect.

---

[78] Robert Pear, *The Nation; Gridlock, the Way It Used to Be*, NY TIMES, Oct. 9, 1994, https://www.nytimes.com/1994/10/09/weekinreview/the-nation-gridlock-the-way-it-used-to-be.html.

[79] *Telecommunications Act of 1996*, FCC, June 20, 2013, https://www.fcc.gov/general/telecommunications-act-1996.

[80] *Modernizing the Electronic Communications Privacy Act (ECPA)*, ACLU, https://www.aclu.org/issues/privacy-technology/internet-privacy/modernizing-electronic-communications-privacy-act-ecpa (last visited Sept. 25, 2018).

[81] *What's new in Gmail*, GOOGLE, https://support.google.com/a/answer/7684334?hl=en (last visited Sept. 25, 2018).

[82] Matt Swinder, *iOS 12: new features and the iOS 12.1 release date*, TECHRADAR, Sept. 24, 2018, https://www.techradar.com/news/ios-12.

[83] *E.g.* INTERNET ASSOCIATION, IA PRIVACY PRINCIPLES FOR A MODERN NATIONAL REGULATORY FRAMEWORK (2018); U.S. CHAMBER, PRIVACY PRINCIPLES (2018).

Similarly, federal comprehensive privacy legislation must take into account all of ways in which data are used, misused, and abused to consumers' detriment – including those uses that may arise in the future – and cannot be confined to addressing solely financial harm and physical injury.[84]

In addition, federal comprehensive privacy legislation must include the privacy interventions articulated in response to the FTC's question about "[w]here . . . interventions [should] be focused [and] what interventions are appropriate."[85]

And, comprehensive privacy legislation must provide for robust accountability measures, including the following:

1. *Ending Forced Arbitration*

When there is unauthorized access to personal information, individuals must be made whole to the greatest extent possible. There are two major barriers to this. The first is the Federal Arbitration Act, which requires courts to honor the forced arbitration clauses in contracts, including forced arbitration clauses buried in the fine print of terms of service agreements. Forced arbitration clauses require consumers to settle any dispute they have with an entity by arbitration rather than having their day in court – and often consumers do not even know an arbitration clause is in their contract until they go to sue. This presents three problems: 1) Arbitrators are often more sympathetic to large entities, who are repeat players in the arbitration system, than most juries would be. 2) Arbitration creates no legal precedent. 3) Frequently, it is not cost-effective for an individual to bring a claim against a large company by herself. The damages she could win likely would not exceed her legal costs. But, when customers can band together in a class action lawsuit, it becomes much more feasible to bring a case against a large entity engaged in bad behavior. Forced arbitration clauses preclude class action. A new privacy regime should explicitly exempt cases addressing the failure to protect personal information from the Federal Arbitration Act to make sure consumers can have their day in court when their information is misused and their trust abused.

2. *Liquidated Damages*

The second major barrier to meaningful recourse is the difficulty calculating the damages associated with unauthorized access to personal information. While one may be able to quantify her damages when her credit card information is breached or her identity is stolen, it is much harder to do so in a situation like Facebook/Cambridge Analytica. It is difficult to put a dollar amount on having one's privacy preferences ignored or her personal information revealed to third-parties without her knowledge or consent. We instinctively know that there is harm in having one's personal data used for "psychographics" to influence her behavior in the voting booth, but that harm is difficult to quantify. Congress already uses liquidated damages in other situations when the damage is real, but hard to quantify. In fact, liquidated damages are already used to address other

[84] For a more fulsome discussion, *see* pp. 6 – 7 *supra*.
[85] *See* pp. 7 – 11 *supra*.

privacy harms. For example, the Cable Privacy Act provides for liquidated damages when cable companies impermissibly share or retain personally identifiable information.[86]

While the FTC can step in when companies engage in unfair and deceptive practices, the FTC is likely to only intervene in the most egregious cases. Moreover, the FTC can only extract damages from companies once they have violated users' privacy once, entered into a consent decree with the Commission, and then violated the consent decree. That means a lot of consumers must have their personal information abused before a company is held to account. Moreover, when the FTC is involved, any damages go to the government, not to making individuals whole.

We are not recommending that the FTC be taken out of the business of protecting consumers in the digital age – in fact, we believe that any comprehensive privacy legislation must strengthen the FTC and provide it with rulemaking authority. We are merely suggesting that consumers should also have the opportunity to protect themselves. Allowing private, class action lawsuits for liquidated damages when companies fail to safeguard private information will create the necessary incentives for entities to take appropriate precautions to protect the information they have been entrusted with. Entities, after all, understand the technology and the risks and are in the best position to develop safeguards to protect consumers.

3. Strong Agency Oversight and Enforcement

Any privacy regime must also be enforced by a strong oversight agency with sufficient resources and rulemaking authority, as described above.

4. State Innovation and Enforcement

While the federal government should set minimum standards of protection for all Americans, states have been in the vanguard of privacy protection and are much-needed cops on the beat. Even if Congress were to dramatically expand the resources available to federal privacy agencies, the federal government could not hope to provide adequate protection to consumers on its own. For example, the FTC is unlikely to get involved in a data breach affecting consumers in just one state. In fact, Massachusetts Assistant Attorney General Sara Cable recently testified that less than one percent of data breaches in Massachusetts affect more than 5,000 people.[87] It is difficult to imagine federal resources being used to investigate a data breach of this size, but a state like Massachusetts might choose to get involved. In fact, Massachusetts is likely to set a breach notification standard that is more appropriate for its state than the federal government might set. For this reason, the states, as laboratories of democracy, should be empowered to innovate and provide greater privacy protections to their residents.

Furthermore, comprehensive privacy legislation must eschew federal preemption. The states have always served as the laboratories of democracy, legislating to address the particular needs of their residents. In addition, entities are accustomed to innovating in an environment with

---

[86] 47 U.S.C. § 551(f)(2)(A) (2001).

[87] *Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime Before H. Comm. on Financial Services, Subcomm. on Financial Institutions and Consumer Credit*, 115th Cong. (2018) (statement of Sara Cable, Assistant Attorney General, Massachusetts).

"a patchwork of competing and contradictory baseline laws."[88] For example, each state has its own banking laws,[89] commercial code,[90] and environmental laws.[91] And, in Europe, GDPR is enforced by twenty-eight different member countries, each with its own implementing regulations.[92] There is no principled reason why consumer privacy should be treated differently.

Finally, as described above, comprehensive privacy legislation must build on the existing sectoral privacy laws and maintain FCC enforcement authority over ISPs and communications networks.

- **Should the FTC have additional tools, such as the authority to seek civil penalties?**

Yes, the FTC requires additional rules, including civil penalty authority, as well as additional tools, such as rulemaking authority,[93] to protect consumer privacy in the digital age. Civil penalty authority may incentivize companies to engage in better privacy practices at the outset if they run the risk of substantial fines for a first violation.

Similarly, APA rulemaking authority will allow for legal clarity while maintaining the flexibility required for privacy protections to keep pace with technological innovation.

- **How should First Amendment norms be weighed against privacy values when developing a legal framework?**

The First Amendment articulates fundamental American rights around freedom of expression and access to information. No right to deletion should be interpreted in a way that would allow individuals to distort the public record or restrict the ability of journalists and others to report on public figures or matters of general interest. At the same time, personal data is not, by itself, a form of "speech," and the First Amendment does not protect the day-to-day, non-expressive business activities of companies that collect, use, or traffic in user data.

Conclusion

We appreciate the opportunity to comment on the FTC's Request for Public Comments Docket No. FTC-2018-0098: Hearings on Competition and Consumer Protection in 21st Century: Consumer Privacy, February 12-13, 2019 and stand ready to assist the FTC as it prepares for the February consumer privacy hearings.

---

[88] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48602 (Sept. 26, 2018).

[89] *See* JAY B. SYKES, CONG. RESEARCH SERV., R45081, BANKING LAW: AN OVERVIEW OF FEDERAL PREEMPTION IN THE DUAL BANKING SYSTEM (2018).

[90] *Commercial Law by State*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/table_commercial (last visited Nov. 2, 2018).

[91] *Environmental Health State Bill Tracking Database*, NAT'L CONF. OF STATE LEGISLATORS (Oct. 19, 2018), http://www.ncsl.org/research/environment-and-natural-resources/environmental-health-legislation-database.aspx.

[92] *See Art. 68 GDPR European Data Protection Board*, INTERSOFT CONSULTING, https://gdpr-info.eu/art-68-gdpr/ (last visited Nov. 2, 2018).

[93] *See* pp. 16 – 17 *supra*.

Sincerely,

Allison S. Bohm
Policy Counsel
Public Knowledge

Appendix A:

Gus Rossi, *Is the GDPR Right for the United States?*, PUBLIC KNOWLEDGE, Apr. 9, 2018, https://www.publicknowledge.org/news-blog/blogs/is-the-gdpr-right-for-the-united-states

Public Knowledge

BLOGS

Is the GDPR Right for the United States?

By Gus Rossi

April 09, 2018 Privacy, Cybersecurity, Security, Data Protection, GDPR

Europe's new privacy law, the General Data Protection Regulation (GDPR) will enter into force in May 2018. Understandably, given that data breaches and privacy violations have been in the headlines lately -- and given that the GDPR will reshuffle privacy protection in Europe and beyond -- many in the United States are looking to the GDPR for ideas of what to do - and what not to do. We think that it would be impractical and ineffective to copy and paste the GDPR to U.S. law -- the institutions and legal systems are just too different.

However, here are some aspects of the GDPR that we think Congress should pay attention to when thinking about how to protect Americans' privacy. It is important to remember two things when thinking about the GDPR and internet platforms. First, the GDPR has not been implemented yet. It will likely take years to see the full extent of its consequences and effects. Second, there is another piece of legislation, the ePrivacy Regulation, which clarifies the consequences of the GDPR for electronic communications, that is still in the European legislative process. We expect the ePrivacy Regulation to be approved before the end of 2019.

(Please also keep in mind that this blog post does not intend to be an exhaustive guide to the GDPR -- it's a long law! -- and that elsewhere, we published our long read on Principles for Privacy Legislation.)

Here are the aspects of the GDPR that we think Congress should consider:

-A definition of personal data (article 4). Even if the transposition of the GDPR's definition of personal data to U.S. law might be impractical, it should start with assuming personal data is "any information relating to an identified or identifiable natural person." Naming the most relevant pieces of information that constitute personal data (the GDPR chooses name or "an identification number," among others) is also a useful baseline for the U.S. Article 9 of the GDPR establishes a different set of conditions for the processing of "special categories of personal data," including but not limited to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or sexual orientation.

-**Emphasis on consent.** Article 4 of the GDPR defines consent as a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Article 7 of the GDPR outlines the conditions for consent. Explicit, clear, granular, and informed consent should be a key part of any U.S. privacy law. Consumers should be clearly informed of what is going to happen to their personal data. If the GDPR is implemented as expected, users will have to explicitly and in a clearly informed way agree to share their data with third parties, especially data brokers. Many will probably agree to share their data. But they will have a clear option to say no.

Consent can be withdrawn at any time. In addition, Recital 43 specifies that consent is not clearly given and therefore invalid if it is made contingent for the provision of a service for which a specific category of personal data is not necessary -- in other words, organizations cannot impose consent to unnecessary data sharing for a provision of a service that does not require such data to function.

-**Non-consent based lawful processing.** Organizations should *sometimes* be allowed to process data without consent, given narrow and specific circumstances (Article 6). The GDPR allows for some other instances where an organization could collect and process personal data without consent, such as the legitimate interest of processing a contract or guaranteeing network security. Recitals 47, 48, and 50 deal with legitimate interest.

-**Pseudonymous data** (article 4 and recital 28). The GDPR defines pseudonymization as the "processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information" and recognizes the ability of pseudonymization to help protect the rights of individuals while also enabling data utility. Pseudonymization may facilitate data processing beyond original collection purposes and scientific research. Likewise, it is also important to know that organizations will not need to

guarantee individual users rights if the data no longer identifies to a specific individual. *Anonymous* data falls out of the scope of the GDPR (Recital 26). Like the GDPR, Congress should consider incentivizing the pseudonymization and anonymization of personal data.

-**Data minimization** (article 5). The GDPR establishes that data processing should only use as much data as is required to successfully accomplish a given task. In addition, the GDPR clarifies that data collected for one purpose cannot be repurposed without further consent.

Congress should encourage incentives to change data collection in America from "collect first, think of uses later" to "think uses first, design collection mechanisms later."

-**Listing user rights** (chapter 3). In the digital era, it is important that consumers know their rights in regards to their personal data. We do not think that all the rights outlined in the GDPR are desirable, and we are particularly wary of the the Right to be Forgotten (article 17), as we are afraid it can easily be abused against the public interest -- for example by a corrupt politician running for reelection to eliminate public information regarding his or her wrongdoings.

There are other rights from chapter 3 that Congress should consider importing with translation, particularly:

1) The right to data portability (article 20) would increase transparency and user control by obliging platforms to share with their users in a machine-readable format the personal data that platforms have collected about a specific user. It is important to keep in mind that while the right to data portability might increase platform competition, this would be a by-product of the GDPR. In fact, in their guidelines for understanding the right to data portability, EU privacy authorities write that "the GDPR is regulating personal data and not competition."

2) The right to transparent information (article 12) establishes that organizations must inform individuals "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child" when their data is being collected. Empowering users starts with clear information.

3) The right to be informed and to access (articles 13, 14, 15): individuals have the right to be informed about the collection and use of their personal data. If an organization obtains data from other sources, it must provide individuals with information regarding the uses and management of that data within one month.

4) Rights related to automated decision-making, including profiling, (article 22) are designed to protect individuals when organizations are undertaking automated decision-making processes

that carry legal or other significant effects on them. The GDPR asks organizations to give individuals information about the processing, allow consumers to request human intervention or challenge a decision, and regularly verify that the systems are working as intended.

5) The right to object to data processing (article 21) will allow Europeans to object to data processing (for example for direct marketing purposes).

-**Mandating independent supervisory authorities** (article 6). Each EU country has one or more independent Data Protection Agencies (DPAs) in charge of the overseeing the implementation and the enforcement of the GDPR. The European Data Protection Agencies have been central for the development of a culture of data protection in Europe and the update of privacy laws across Europe.

The U.S. does not necessarily need to copy the European institutional framework. But something is clear: one or more agencies must be definitively empowered and equipped to oversee, enforce, and advocate for Americans' privacy rights. The EU institutional framework gives the U.S. another valuable lesson in what regards to decentralization: there is no single EU-wide DPA. Instead, there are many national DPAs. The U.S. should also allow states to explore different ways to guarantee privacy rights. State action preemption is not a condition for privacy rights enforcement. A federal framework and specialized institutions are.

-**Privacy by design and by default** (article 25). Privacy by design establishes that privacy has to be a fundamental consideration from the initial design stages of new products, services, or processes that involve personal data and throughout development. Privacy by default means that the default privacy settings of products or services should be set to the most privacy-friendly levels. These are not new or even European-only principles: Canada is moving towards privacy by design too.

If Congress wishes to be forward looking and encourage innovation that is respectful of privacy, mandating privacy by design and by default is a step in the right direction.

-**Data Protection Impact Assessments** (DPIAs, article 35). Organizations are required to assess and mitigate privacy risks in new data processing activities. This is especially important when a new product is launched or a new technology used. This would help organizations rethink their products before launching them. The GDPR clarifies that DPIAs "shall in particular be required" in case of a "systematic monitoring of a publicly accessible area on a large scale," "[p]rocessing on a large scale of special categories of data or of personal data relating to criminal convictions and offences," or profiling. Given ongoing complaints about racial and other biases in algorithms and machine learning, this risk mitigation could be more important to a multicultural U.S. than the more comparatively homogeneous Europe.

As with privacy by design and by default, DPIAs are safeguards to guarantee that technological innovation will be respectful of privacy. Congress should consider adopting DPIAs in the U.S.

-**Data Protection Officer** (DPO, article 39). DPO a privacy and security leadership role that the GDPR requires basically all organizations processing, controlling, or collecting personal data to have. DPOs are in charge of overseeing an organization's compliance with the GDPR requirements and cooperating with Data Protection Agencies when necessary.

The idea behind the figure of the DPO is to oblige all organizations processing personal data to have someone with knowledge of the law to educate and train data processing employees, to think about data protection, and to dialogue with the authorities. Any company that processes and collects data on a regular basis will have to appoint a DPO. Congress should study whether all small and medium enterprises should be required to have DPOs. But DPOs could create a permeable culture for privacy protection in the U.S.

-**Certification mechanisms** (article 42). The GDPR encourages the creation of EU-level certifications, seals, and marks that companies can earn to demonstrate compliance with the GDPR for some or all of their services or products. This would be particularly useful for consumers, since it would allow them to quickly identify the most privacy protective products and services.

Certifications, seals, and marks would not be a novelty in the U.S. consumer protection landscape. They already exist for chemicals and food. Congress should consider easing consumer understanding of privacy policies, data protection, and security practices by encouraging or mandating certification mechanisms.

-**Data breach notification** (article 33). The GDPR establishes that the organizations that ask consumers for data and establish the purposes and means of processing personal data should notify the relevant DPA of data breaches within 72 hours of occurrence, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Organizations processing data on behalf of other organizations are required to notify the first without undue delay after becoming aware of a personal data breach.

Congress should include data breach notification in any comprehensive privacy bill.

-**Security of processing** (article 32). The GDPR mandates that all organizations handling or requesting personal data “implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk” of the data processing, including using encryption. Congress should also consider security and risk of data breach when thinking of

privacy.

-**Penalties** (chapter 8). Here the principle is simple: any good law needs teeth.

Americans deserve privacy protection. The GDPR outlines some interesting elements for a strong privacy bill. We suggest Congress critically study and understand them. Copying and pasting EU law would not be an efficient or reasonable way to protect Americans' privacy. But there is significant value in looking at examples of how other jurisdictions address policy issues, and in this case is particularly important for a nation in urgent need of data protection reform.

Image credit: Flickr user thedescrier

Share

Facebook

Twitter

Google+

Reddit

Email

Print

More Videos
Videos

A Net Neutrality Christmas Carol
Watch now

Pie for Broadband Monopolies, Crumbs for Consumers
Watch now

Follow Us
Facebook
Twitter
Youtube
Join The Public Knowledge Mailing List
Stay Connected. Stay Informed. Subscribe

Public Knowledge

Public Knowledge promotes freedom of expression, an open internet, and access to affordable communications tools and creative works. We work to shape policy on behalf of the public interest.

Type here to search...

This work is licensed under the Creative Commons Attribution ShareAlike 3.0 License.

Copyright ©2018 Public Knowledge

Privacy Policy | **Contact Us** | **Donate**

Appendix B:

Allie Bohm, *Is California's New Privacy Law Right for the United States?*, PUBLIC KNOWLEDGE, July 16, 2018, https://www.publicknowledge.org/news-blog/blogs/is-californias-new-privacy-law-right-for-the-united-states

Public Knowledge

BLOGS

Is California's New Privacy Law Right for the United States?

By Allie Bohm

July 16, 2018 Privacy, Consumer Privacy, Legislation, Data Protection, California

At the end of June, California enacted what has been billed as a comprehensive privacy law. By all accounts, it was a rush job, negotiated in a week behind closed doors in a desperate and successful attempt to keep Californians for Consumer Privacy Campaign Chairman Alaistair MacTaggart's privacy initiative off the November ballot. As sometimes happens, the law's proponents and a few reporters may have overhyped the legislation – both given its current contents and because many expect it to change before its effective date in January 2020.

Nonetheless, lawmakers in Congress and in states beyond California may be looking to the new law for ideas. Those doing so should take the law as it stands with a grain of salt. Even before the ink dried on the law, stakeholders were promised additional legislation amending the law, and the California Attorney General (AG) is required to promulgate rules enacting the details of the law in 2020. Plus, it's impossible to know what exactly a law will do until it goes into effect and is litigated. But, this blog takes a deep dive into the law and outlines some of the provisions policymakers should keep in mind as they consider which parts of the California law to export:

Room for Improvement:

1) Notice Only: The California law requires businesses to notify Californians, "at or before the point of collection," of "the categories of personal information to be collected and the purposes

for which the categories of personal information" will be used. While transparency is a step in the right direction, this language seems to allow businesses to collect whatever personal information they wish to and use it for whatever purposes they wish – provided they tell you, the consumer, that they are doing it. You do not have the ability to limit data collection or use (although you can require a business to delete your data after the fact – subject to certain limitations – and you can stop a business from selling your data – see further discussion below). This is considerably less protective of consumers than most of the federal proposals on the table. In fact, even the most modest federal bill would allow consumers to limit the collection and use of their personal information.

There is also no reason to believe that this notification requirement, in and of itself, would in any way change current business practices. Businesses already disclose the categories of information they collect and what they use it for in their terms of service – because they are afraid that the Federal Trade Commission (FTC) will come after them under the Agency's deceptiveness authority if they don't. Of course, it would take 76 work days to read all of the privacy policies we encounter in a year, so very few people read those disclosures. Nothing about the California law would change that.

2) Opt-Out for Selling Personal Information: The California law permits (adult) consumers to opt out of the sale of their personal information. This is a step in the right direction, but there are two problems. First, it applies only to the sale of personal information. Now, sale is defined slightly more broadly than it is in the conventional sense, but the definition would not reach the dissemination of personal information when no value is received in exchange – *e.g.* where data are donated for research purposes. It also would not reach advertising practices used by Facebook and other platforms where the personal information itself is not conveyed to the advertiser, but rather the advertiser gives the platform the demographics it wishes to reach, and the platform places the ad by looking at its data itself.

Moreover, the opt-out regime itself is problematic. Too often the default is destiny; most people never change default settings. This means a lot more personal information will be sold under the opt-out regime than would be under an opt-in regime. The problem here? Our personal information is just that – personal. We should be in the position to decide whether it is sold and to whom. (Note: the law does require opt-in consent for the sale of personal information when the Californian is under age 16.)

3) Pay for Privacy: The new law includes a provision that appears at first blush to stop businesses from discriminating against consumers who have asked for their data or prohibited the sale of their data. But, it includes carve-outs that allow businesses to charge different rates, provide different qualities of service, or offer financial incentives to consumers to share or permit the sale of their personal information, so long as the prices or differences are related "to

the value provided to the consumer by the consumer's data." These exceptions are poorly drafted and include conflicting standards, but most readers agree that they permit a business to require you to pay for the value of your data – *i.e.* to pay for your privacy.

Public Knowledge does not oppose pay-for-privacy in all circumstances; however, the inclusion of pay-for-privacy raises some concerns. On the one hand, the ability to exchange some information for something of value is consistent with the philosophical proposition that you own your own data. On the other hand, it may make privacy a luxury good, available only to those who can afford to pay for it, running the very real risk of further marginalizing the most marginalized. This risk is especially high in situations that have traditionally been regarded as coercive to consumers, such as "take it or leave it" offers or where essential services are involved. Additionally, Public Knowledge has urged that even where a person consents to the collection and use of personal information, that person should retain an ongoing right to withdraw consent. The California law does not clearly contain such safeguards or a clear right to withdraw consent; this clause requires significant improvement in future legislation or regulations or the carve outs should be removed entirely.

Lesser Strengths:

1) Data Portability: The California law requires data portability, giving Californians the right to request "the categories and specific pieces of personal information the business has collected." Businesses that receive a "verifiable" request must provide the requested information to the consumer within 45 days, with extensions allowed. This promotes competition and consumer choice by allowing consumers to take their information to competing services or websites.

If a business provides the personal information electronically, the information must be in a machine-readable format. But, the business is also permitted to provide the information in paper copy, which would make it infinitely less portable.

Moreover, businesses are only required to disclose personal information from the previous 12 months. When many consumers have multi-year relationships with businesses, this would only require the return of a fraction of their personal information.

2) Right to Be Forgotten: The California law contains an Americanized version of the Right to Be Forgotten, although the law's deletion right only applies to information the consumer herself has provided to the business. Unlike its European counterpart, the California version has a carve-out to ensure that others are able to exercise their First Amendment right to access information.

Unfortunately, the First Amendment carve-out is only one of nine exceptions to the deletion requirement. Three of the other exceptions, which pertain to the maintenance of information that is "reasonably anticipated" by consumers or "reasonably aligned" with consumer expectations of their relationship with the business or "compatible with the context in which the consumer provided the information" would probably exempt certain platforms from having to fully delete any consumer data ever. After all, aren't an advertisement-supported platform's business relationship with the consumer and the consumer's expectation of that business relationship both that the platform will gobble up all of her information?

3) Applicability: California's law applies to all businesses that meet certain thresholds. The good is that the law does not differentiate between online businesses and brick-and-mortar businesses that collect consumer information through loyalty cards or other mechanisms. The bad is that it applies only to businesses and not to nonprofits or other non-business entities that collect consumer data. It is also unclear whether the statutory thresholds are the right thresholds.

4) Private Right of Action: The California law contains a private right of action for data breach, and that private right comes with liquidated damages. Unfortunately, the circumstances where the private right would apply are vanishingly small. Indeed, Californians can only take advantage of the private right when a very short list of non-encrypted or non-redacted identification information and account numbers are exfiltrated, stolen, or disclosed. This is a much smaller subset of the personal information that is purported to be protected by the rest of the California law and perpetuates the antiquated sensitive/non-sensitive distinction in U.S. privacy law. And, if the personal information was inadequately encrypted or redacted, it seems that the private right does not apply at all. Rather, companies with inadequate security practices are given a free pass. In fact, the amendment history for the law makes clear that this provision was meant to limit the private right as much as possible.

The law also allows the California AG broad authority to halt consumer lawsuits, even when the AG refuses to take up the case.

The law's notice and opt-out requirements are enforceable only by the state AG, who can bring an action for civil penalties. Those penalties cap out at $7,500 per violation.

Strengths:

1) Ban on Tertiary Sale of Personal Data: The new law prohibits businesses that have purchased Californians' personal information from selling it to another party without notifying the individual consumer and giving him/her the opportunity to opt-out. While opt-in consent would be stronger, this could put a dent in the resale marketplace for personal information and

help Californians better keep tabs on who has information about them.

2) You Don't Have to Have an Account to Take Advantage of California's Privacy Law: Given the proliferation of integrated social media "like" and "share" buttons – basically third party trackers – across the internet, one of the trickiest issues facing lawmakers seeking to legislate privacy in the digital age is how to address the privacy of individuals who have never opted in to having a relationship with a business by creating an account. The California law tackles this problem by mandating that consumers be permitted to request their personal information from a business and prohibit the sale of their personal information without creating an account with the business.

3) Making It Easy to Opt Out: While it would be better to require opt-in consent, at least the California law requires that the link to opt out of personal information sale be "clear and conspicuous" and use the standard language, "Do Not Sell My Personal Information." The law further requires the state AG to develop "a recognizable and uniform opt-out logo or button." Having a consistent logo across websites will make it easier for Californians to vindicate their opt-out rights – they will know what to look for and won't have to poke around for a different logo on each website.

4) Eliminating the Sensitive/Non-Sensitive Distinction: California's law seems to eliminate, at least for the notice and opt-out requirements, the sensitive/non-sensitive distinction that has been present in many privacy laws and bills in the past. This distinction, which grants greater protection to purportedly sensitive information, like first and last name, social security numbers, bank account numbers, than to so-called non-sensitive information, is increasingly illogical in today's world. Indeed, under the old world order, the personal information in question in Facebook/Cambridge Analytica – information like social media "likes" that may be useful for influencing an individual in the voting booth, as well as for more mundane marketing and advertising purposes, and that, when aggregated, may, in fact, be personally identifiable – would not be considered sensitive and would not be protected. The California law does away with this archaic distinction by simply defining "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The law does include an illustrative, non-exhaustive list of personal information, and, helpfully, that list includes "*[i]*nferences drawn" about a consumer.

The law also orders the state AG to promulgate regulations adding categories of information to the enumerated list in order to ensure that the law keeps pace with technology. But some readers have felt that the inclusion of a list raises the question of whether the law in fact does away with the sensitive/non-sensitive distinction.

The California law adopts some other useful definitions and concepts from the EU's General Data Protection Regulation. For example, the law clarifies that in order to qualify as "deidentified" information, the business that maintains the information must have implemented technical safeguards, as well as business practices and processes, to prohibit reidentification.

5) Preventing Work-Arounds: California's law helpfully voids any contract that purports to sign away consumers' rights under the law and also includes language making clear that if a company takes a bunch of convoluted steps with personal information in order to evade the law's requirements, a court enforcing the law must ignore the convoluted steps.

All Americans deserve privacy protection. There are a few ideas federal lawmakers (and other state lawmakers) might want to crib from California, but federal policy makers should set a higher floor for federal protections. It sounds like California's lawmakers will be reopening this law again before it goes into effect in two years. They should use the opportunity to strengthen its consumer protections.

Image credit: Flickr user opensourceway

Share

Facebook

Twitter

Google+

Reddit

Email

Print

More Videos
Videos

A Net Neutrality Christmas Carol
Watch now

Pie for Broadband Monopolies, Crumbs for Consumers
Watch now

Follow Us
Facebook
Twitter
Youtube
Join The Public Knowledge Mailing List
Stay Connected. Stay Informed. Subscribe

Public Knowledge

Public Knowledge promotes freedom of expression, an open internet, and access to affordable communications tools and creative works. We work to shape policy on behalf of the public interest.

Type here to search...

This work is licensed under the Creative Commons Attribution ShareAlike 3.0 License.

Appendix C:

PUBLIC INTEREST PRIVACY PRINCIPLES (2018)

Public Interest Privacy Legislation Principles

Unregulated data collection and use in the United States has eroded public trust in companies to safeguard and use data responsibly. Surveys show that, while individuals often try to remove or mask their digital footprints,[1] people think they lack control over their data,[2] want government to do more to protect them,[3] and distrust social media platforms.[4]

The current U.S. data privacy regime, premised largely upon voluntary industry self-regulation, is a failure. Irresponsible data practices lead to a broad range of harms, including discrimination in employment, health care, and advertising, data breaches, and loss of individuals' control over personal information. Existing enforcement mechanisms fail to hold data processors accountable and provide little-to-no relief for privacy violations.

The public needs and deserves strong and comprehensive federal legislation to protect their privacy and afford meaningful redress. Privacy legislation is essential to ensure basic fairness, prevent discrimination, advance equal opportunity, protect free expression, and facilitate trust between the public and companies that collect their personal data. Legislation should reflect at least the following ideas and principles:

1. Privacy protections must be strong, meaningful, and comprehensive

Privacy concerns cannot be fully addressed by protecting only certain classes of personal data held by some companies. Legislation should mandate fairness in all personal data processing, respect individuals' expectations for how data should be treated, provide for data portability, and include safeguards against misuse of data, including de-identified and aggregate data. Legislation should advance fundamental privacy rights and require all entities that collect, store, use, generate, share, or sell (collectively, "process") data both online and offline to comply with Fair Information Practices[5] (collection limitation, data

---

[1] *The State of Privacy in Post-Snowden America*, Pew (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america. +

[2] Bree Fowler, *Americans Want More Say in the Privacy of Personal Data*, Consumer Reports (May 18, + 2017), https://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data. +

[3] Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, Pew (Mar. + 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns. +

[4] *Id.* $

[5] Fair Information Practices are similar to those adopted by the OECD. *See* OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. +

quality, purpose specification, use limitation, security safeguards, openness, access and correction rights, and accountability) across the complete life cycle of the data. Legislation should require all data processing to be clearly and accurately explained, justified, and authorized by the individual. People should have the right to know when their data has been compromised or otherwise breached. Additionally, legislation should require entities processing data to adopt technical and organizational measures to meet these obligations, including risk assessments of high-risk data processing.

2. Data practices must protect civil rights, prevent unlawful discrimination, and advance equal opportunity

Legislation should ensure fundamental fairness of and transparency regarding automated decision-making. Automated decision-making, including in areas such as housing, employment, health, education, and lending, must be judged by its possible and actual impact on real people, must operate fairly for all communities, and must protect the interests of the disadvantaged and classes protected under anti-discrimination laws. Legislation must ensure that regulators are empowered to prevent or stop harmful action, require appropriate algorithmic accountability, and create avenues for individuals to access information necessary to prove claims of discrimination. Legislation must further prevent processing of data to discriminate unfairly against marginalized populations (including women, people of color, the formerly incarcerated, immigrants, religious minorities, the LGBTQIA/+ communities, the elderly, people with disabilities, low-income individuals, and young people) or to target marginalized populations for such activities as manipulative or predatory marketing practices. Anti-discrimination provisions, however, must allow actors to further equal opportunity in housing, education, and employment by targeting underrepresented populations where consistent with civil rights laws. Moreover, decades of civil rights law have promoted equal opportunity in brick-and-mortar commerce; legislation must protect equal opportunity in online commerce as well.

3. Governments at all levels should play a role in protecting and enforcing privacy rights

The public consistently call for government to do more, not less, to protect them from misuse of their data. Legislation should reflect that expectation by providing for robust agency oversight, including enhanced rulemaking authority, commensurate staff and resources, and improved enforcement tools. Moreover, no single agency should be expected to police all data processors; therefore, legislation should empower state attorneys general and private citizens to pursue legal remedies, should prohibit forced arbitration, and importantly, should not preempt states or localities from passing laws that establish stronger protections that do not disadvantage marginalized communities.

4. Legislation should provide redress for privacy violations

Individuals are harmed when their private data is used or shared in unknown, unexpected, and impermissible ways. Privacy violations can lead to clear and provable financial injury, but even when they do not, they may, for example, cause emotional or reputational harm; limit awareness of and access to opportunities; increase the risk of suffering future harms; exacerbate informational disparities and lead to unfair price discrimination; or contribute to the erosion of trust and freedom of expression in society. In recognition of the many ways in which privacy violations are and can be harmful, legislation should avoid requiring a showing of a monetary loss or other tangible harm and should make clear that the invasion of privacy itself is a concrete and individualized injury. Further, it should require companies to notify users in a timely fashion of data breaches and should make whole people whose data is compromised or breached.

Signed,

Access Humboldt
Access Now
Berkeley Media Studies Group
Campaign for a Commercial-Free Childhood
Center for Democracy & Technology
Center for Digital Democracy
Center for Media Justice
Center on Privacy & Technology at Georgetown Law
Color of Change
Common Cause
Common Sense Kids Action
Consumer Action
Consumer Federation of America
Consumers Union
Customer Commons
Demand Progress
Free Press Action Fund
Human Rights Watch
Lawyers' Committee for Civil Rights Under Law
Media Alliance
Media Mobilizing Project
National Association of Consumer Advocates
National Consumer Law Center
National Consumers League
National Digital Inclusion Alliance
National Hispanic Media Coalition
New America's Open Technology Institute
Oakland Privacy
Open MIC (Open Media and Information Companies Initiative)
Privacy Rights Clearinghouse
Public Citizen
Public Knowledge
U.S. PIRG
United Church of Christ, OC Inc.