NISKANEN CENTER

Regulatory Comment

Comments submitted to the National Telecommunications and Information Administration in the Matter of:

REQUEST FOR COMMENTS ON DEVELOPING THE ADMINISTRATION'S APPROACH TO CONSUMER PRIVACY

Alec Stapp
Technology Policy Fellow
Niskanen Center

Ryan Hagemann
Senior Director for Policy
Niskanen Center

Submitted: November 8, 2018
Docket Number: 180821780-8780-01

EXECUTIVE SUMMARY

Contrary to the popular narrative, most Americans do not place a high value on their privacy. Indeed, most are either "privacy pragmatists" or "privacy unconcerned." Only a minority are "privacy fundamentalists" — that small subset of the population that claims they would never trade their privacy for economic benefits. The majority of Americans, in fact, are continually evaluating the trade-offs associated with sharing private information, using simple heuristics to make those choices. Nonetheless, the media and activists continue to push a misleading narrative that does a great disservice to evidence-based policy debates. As a result, policymakers now face a choice between pursuing policies that prioritize pragmatic governance of consumer privacy — and the economic growth such an approach engenders — or embarking on an experiment with the failed European model of regulating privacy using prescriptive mandates.

The privacy regulation model the United States has followed in recent decades for non-sensitive data — known as "notice and choice" or "notice and consent" — has not been perfect, but it has successfully balanced privacy and economic concerns. This minimalist, consistent, and simple legal environment for commerce has been a significant reason why the United States remains the leader in the digital economy. Europe, on the other hand, has taken increasingly draconian approaches to privacy regulating, beginning with the adoption

of the Data Protection Directive in 1995 and brought to more onerously restrictive regulatory heights with the implementation of the General Data Protection Regulation earlier this year.

Federal baseline privacy rules are urgently needed to prevent a patchwork of state and local privacy regulations from choking off innovation in the digital economy. In deciding how to structure these rules, the National Telecommunications and Information Administration should review the evidence of the costs and benefits of the current informal notice and choice model. Any future regulatory framework should include prioritizing the following outcomes: transparency, security, risk management, and accountability.

Rules that require firms to minimize data collection or afford users broad rights to access and correction of their information may sound appealing in theory, but impose immense costs, produce a litany of unintended consequences, and slow economic growth and innovation. Data minimization requirements, access and correction rights, opt-in mandates, and other prescriptive rules won't significantly improve consumer privacy outcomes; instead, they will merely cement the likelihood that the United States gives away its position to China as the world's preeminent innovation-based economy, while joining the digital basket case that is the European Union.

INTRODUCTION

In the 1990s, famed privacy scholar Alan Westin developed his Privacy Segmentation Index (PSI) to classify people in three broad categories: "privacy pragmatists," "privacy unconcerned," and "privacy fundamentalists." Westin used answers to privacy-related questions in a short survey to categorize respondents. According to this taxonomy, privacy fundamentalists believe that people should refuse to share private information with businesses and that the government should enact strong regulations to control privacy. The privacy unconcerned see little problem in sharing information with almost any business and think the government should stay out of this domain.

Privacy pragmatists — the largest group in almost every survey since its inception — weigh the economic benefits of disclosing private information against the risks of doing so with a specific organization in a particular context. They generally favor voluntary privacy standards and consumer choice but are not opposed to regulatory intervention if standards are not being met. While more recent research has criticized the broadness of these categories — arguing that privacy is context-dependent — the PSI continues to be used by researchers today, making it a valuable tool for tracking changes in the public's general privacy attitudes over time.

In Exhibit A, we have collected results from nine Westin PSI surveys between 1995 and 2014. In 2001 Congressional testimony, Westin summarized his research (to that point) by noting that despite privacy concerns, "American consumers, by large majorities, want all the benefits and opportunities of a consumer service society and of a market-driven social system."[1] He went on to compare American attitudes toward privacy to those in the Europe: "We know that a majority of the American public does not favor the European Union style of omnibus national privacy legislation and a national privacy regulatory agency, but when it comes to sensitive information such as financial information or health information, overwhelming majorities are looking to legislative protections to set the rules and the standards for that kind of activity."[2]

Looking across the PSI surveys from before and after Westin's 2001 testimony, not much has changed in Americans' attitudes and preferences for privacy. Between one-fourth and one-third of Americans are privacy fundamentalists, about half to two-thirds are privacy pragmatists, and less than one-tenth are privacy unconcerned. In other words, a consistent majority of Americans will either readily give up data about themselves in exchange for economic benefits or pragmatically weigh the risks and benefits of sharing private information with companies on a case-by-case basis. Only a small minority of Americans is presumptively distrustful of sharing private information, always choosing privacy controls over economic benefits.

Sector-based privacy rules have worked well for the United States and do not require drastic changes. Courtesy of Alan McQuinn, a senior policy analyst at the Information Technology and Innovation Foundation, Exhibit B shows the range of U.S. privacy laws that govern the collection and use of various types of consumer data (both sensitive and non-sensitive), based on the industry or sector doing the collection and on the age of the individual (with special protections for children).[3]

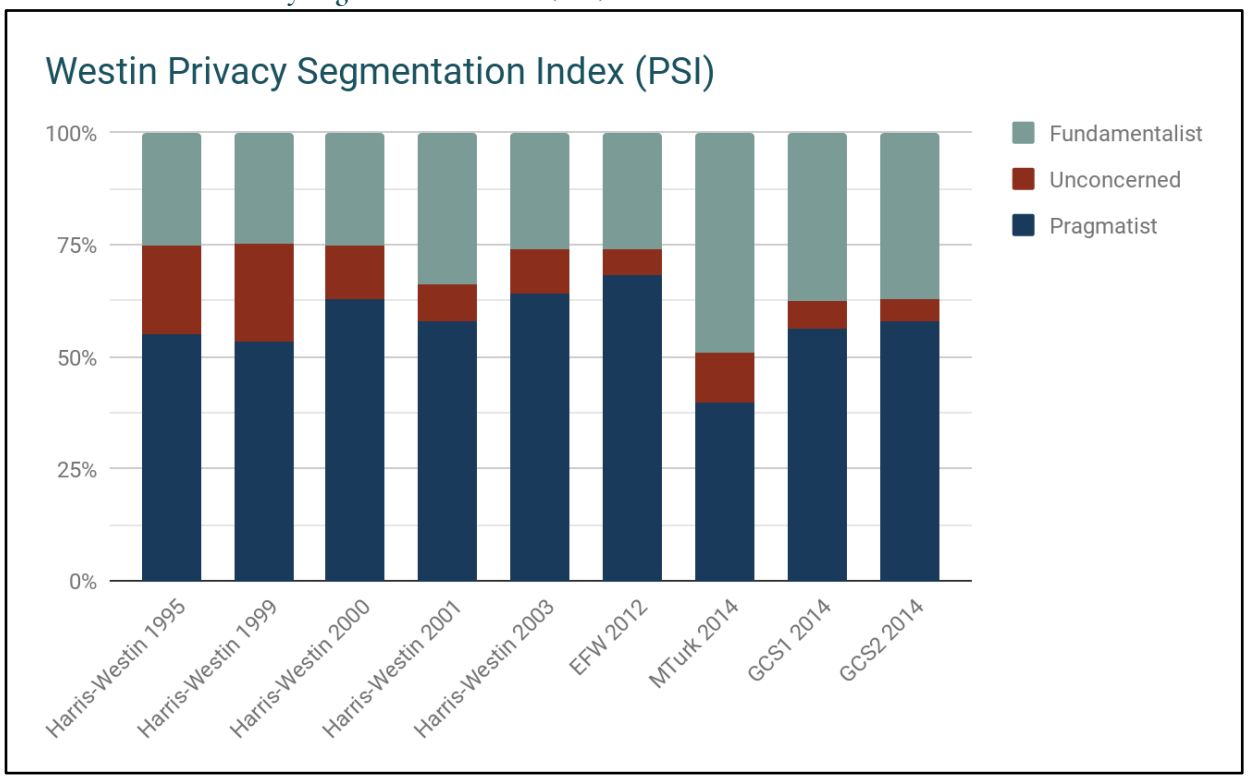
---

[1] Statement of Alan F. Westin, Hearing before the Subcommittee on Commerce, Trade and Consumer Protection of the Committee on energy and Commerce, House of Representatives, "Opinion Surveys: What Consumers Have to Say About Information Privacy," 107th Congress, 8 May 2001, https://www.gpo.gov/fdsys/pkg/CHRG-107hhrg72825/html/CHRG-107hhrg72825.htm.

[2] *Id.*

[3] Alan McQuinn, "Uncerstanding Data Privacy," *RealClearPolicy*, 25 Oct. 2018, https://www.realclearpolicy.com/articles/2018/10/25/understanding_data_privacy_110877.html.

Exhibit A: Westin Privacy Segmentation Index (PSI)



Sources: "Privacy indexes: a survey of Westin's studies," http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf; "Choice Architecture and Smartphone Privacy: There's A Price for That," https://www.guanotronic.com/~serge/papers/weis12.pdf; "Would a privacy fundamentalist sell their DNA for $1000 ... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences," https://www.usenix.org/system/files/conference/soups2014/soups14-paper-woodruff.pdf.

Exhibit B: U.S. Sector- and Age-Based Privacy Laws

Federal Law	Type of Data Protected
Health Insurance Portability and Accountability Act (HIPAA)	Personal medical data held by hospitals, physicians, and other entities.
Gramm-Leach-Bliley Act (GLBA)	Personal financial information held by financial services firms.
Fair Credit Reporting Act (FCRA)	Consumer credit data held by reporting agencies.
Communications Act	Consumer network information held by telephone companies.
Family Educational Rights and Privacy Act (FERPA)	Education records maintained by education institutions.
Video Privacy Protection Act (VPPA)	Personal informational for rentals of videos, video games, etc.
Data Privacy Act	Data acquired by electronic data recorders in automobiles.
Children's Online Privacy Protection Act (COPPA)	Personal data of children under the age of 13 that is collected online.

PART I: AGAINST PRIVACY FUNDAMENTALISM

A. Through this RFC, the Department is first seeking feedback on what it believes are the core privacy outcomes that consumers can expect from organizations.

1. **Are there other outcomes that should be included, or outcomes that should be expanded upon as separate items?**
2. **Are the descriptions clear? Beyond clarity, are there any issues raised by how any of the outcomes are described?**
3. **Are there any risks that accompany the list of outcomes, or the general approach taken in the list of outcomes?**

In passing the General Data Protection Regulation (GDPR) — which continues to impose significant costs on businesses and consumers for dubious privacy gains — the European Union (EU) made clear its preference for the privacy fundamentalist approach. The omnibus law embraces that worldview by arguing that privacy is a right that trumps the rights to free speech, economic liberty, and the fundamental right of individuals to contract with one another, which restricts EU citizens' ability to exchange their personal information to satisfy other desires.

We agree that privacy is a human right. In the United States, the right to privacy is implicit in the Third, Fourth, and Fifth Amendments in the Constitution. However, as Eli Noam, professor of finance and economics at Columbia University, aptly notes:

> *A right is merely an initial allocation. It may be acquired without a charge and be universally distributed regardless of wealth, but it is in the nature of humans … to exchange what they have for what they want. … Whether we like it or not, people continuously trade in rights.*[4]

As we emphasized in recent comments to the Federal Trade Commission (FTC), even though the organizations espousing privacy fundamentalist beliefs "tend to be louder and more emotionally forceful than others, the shrillness with which a conviction is proclaimed is not dispositive of some manifest truth; merely disputing the absolute sacrosanctity of privacy does not imply a cavalier indifference to its value."[5]

Unfortunately, those shrill voices have already found some success in importing EU-style regulation to American shores. With the recent passage of the California Consumer Privacy Act (CCPA), there is now an urgent need for policymakers to begin considering how best to craft federal baseline privacy rules to create a harmonized — but innovation-friendly — regulatory landscape. These rules will require preempting state and local regulations to prevent the emergence of a patchwork of red tape that will slow innovation, investment, and job growth to a snail's pace — when moving through molasses.

In the next section, we will discuss the various "rights" that are commonly invoked by privacy fundamentalist advocates in their domestic and foreign crusade to impose a one-size-fits-all vision of privacy governance. We will then consider which of these "rights" may be necessary for achieving the core privacy outcomes NTIA describes.

---

[4] Eli M. Noam, "Privacy and Self-Regulation: Markets for Electronic Privacy," in Privacy and Self-Regulation in the Information Age, U.S. Department of Commerce, 1997, https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy.

[5] Ryan Hagemann, *Comments to the Federal Trade Commission in the Matter of: Hearings on Competition and Consumer Protection in the 21st Century*, Niskanen Center (Washington, D.C.; 20 Aug. 2018), p. 2, https://niskanencenter.org/wp-content/uploads/2018/08/Comments-Consumer-Welfare-Implications-of-AI-FTC.pdf.

A. Data Protection: The Good, the Bad, and the Ugly

While some data rights in the GDPR are sensible, reasonable, and minimal ("The Good") — and therefore appropriate — others are either redundant or too ambiguous to achieve their ends ("The Bad"), or pose the risk of producing too many unintended consequences ("The Ugly"). These comments will use this "rights" terminology to increase clarity and ease international comparisons. However, it is important to remember that shared terminology matters less than shared principles. As independent privacy counsel Paula Bruening has noted, "Traditional notions of fair information practices bridge differing approaches to privacy protection by serving as a common language for privacy."[6] In the discussion that follows, we will cite evidence from the recent implementation of the GDPR in the EU, as it is a noteworthy change to privacy regulation and can serve as an object lesson for future policymaking.

1. The Good

As a foundation for federal baseline data and privacy regulations, we support a right to transparency (i.e., openness and awareness), a right to notice and opt-out (i.e., choice and consent), and a right to breach notification. All data and privacy rights should fall under a broad umbrella of data accountability. However, there are a number of trade-offs that policymakers need to consider when crafting a framework for data accountability.

First, it is important to note that while there is likely unanimous support for privacy policies that are concise, intelligible, and accessible, in practice these legal notices are often lengthy and detailed to limit liability and ensure follow-through on guarantees. Counterintuitively, a privacy policy that is too short or lacking in specifics may make it more difficult for informed advocates to know how user data is being collected and used, and, therefore, what remedial action might be warranted. Regulatory guidance on transparency should keep these trade-offs in mind.

Second, users of online service providers and platforms should receive notice of privacy policies and have the choice to opt-out of sharing data. (Though users do not have a right, as expressed as a provision under the CCPA, to free ride off others and use services whose business models depend on data collection). Opt-in choice architecture is inferior to opt-out because it is biased toward incumbents. Users might be more willing to affirmatively give consent to businesses they already know, even if a newer company with less brand recognition has the same or better data security practices. Any data accountability frameworks, regulations, or principles should expressly disavow a mandatory default opt-in regime for data collection.

Third, users should have the right to notification in the case of data breaches. However, there are some important caveats. Organizations should not be subject to arbitrarily short disclosure deadlines. As Alex Stamos, a former chief security officer of Facebook, has pointed out, hard-and-fast time rules have unintended consequences.[7] For example, firms are incentivized to announce the maximum number of users potentially impacted, which spreads undue panic before an investigation can determine who — if anyone — was actually harmed. Additionally, notification rules can hinder coordination with law enforcement and prevent opportunities for gathering information material to identifying and punishing those responsible. Notification rules should allow for a reasonable amount of time to investigate the breach and incentivize collaboration and coordination with state and federal law enforcement officials.

---

[6] Paula Bruening, "Fair Information Practice Principles: A Common Language for Privacy in a Diverse Data Environment," *Policy@Intel*, 28 Jan. 2016, https://blogs.intel.com/policy/2016/01/28/blah-2/.

[7] Alex Stamos, Twitter post, 1 Oct. 2018, 8:26 am, https://twitter.com/alexstamos/status/1046783533220421632.

Finally, omnibus privacy rules should include an overarching principle of accountability. If an organization has been entrusted with sensitive data, then it has a duty to follow best practices and standards for risk mitigation and security. In practice, policymakers should avoid pre-determining what constitutes "best practices." A prescriptive approach to data security may minimize the incentives for firms to continually improve their cybersecurity best practices and adopt better technologies, resulting in diminished security — and user trust — over time. Instead, data accountability should focus on holding organizations responsible for the promises they make to users regarding the handling and storage of collected data. Failure to deliver on those promises should be sanctioned by the FTC.

2. The Bad

Data minimization requirements and the purpose-limitation principle would have profoundly negative consequences for innovation and economic growth. Biomedical researchers have voiced concerns that GDPR "will make it harder to share information across borders or outside their original research context."[8] The Danish Cancer Society study that found no link between mobile phone use and cancer rates used data that was initially collected for a different purpose.[9] Under GDPR rules, these types of socially-beneficial and potentially life-saving uses of data would have been forbidden.

While GDPR's predecessor — the 1995 European Directive — allowed companies to charge a small fee to offset the additional administrative compliance costs and prevent spurious requests for data, GDPR requires users to be granted free access to personal information. The former approach, while far from ideal, was superior. In another unintended consequence of the right to access, a hacker got access to someone's Spotify account and was able to demand a file with all of their account data.[10] Users should be allowed to access basic personal information retained by a company so long as the release of such data would not adversely affect the company's intellectual property and the administrative burden on organizations is not disproportionate to consumer interest.

3. The Ugly

The right to be forgotten (RTBF) is in direct conflict with freedom of speech and the public's right to know. Convicted scammers have already exploited this rule to get their criminal histories scrubbed from the Internet.[11] The right of data portability sounds appealing in the abstract but is actually problematic for cybersecurity. Data portability requirements increase what cybersecurity researchers call the "attack surface" of a platform by adding additional attack vectors for bad actors (that is, it increases the number of potential access points a hacker could utilize to gain access to a network). The Cambridge Analytica scandal was a classic example of data falling into the wrong hands because it was too portable. A data portability requirement can also be anticompetitive, as data might get sucked in by Facebook and Google from emerging competitors trying to differentiate themselves.

---

[8] Sarah Wheaton, "5 BIG Reasons Europe Sucks at Curing Cancer," *Politico*, 12 Oct. 2018, https://www.politico.eu/article/cancer-5-big-reasons-europe-sucks-at-curing/.

[9] Patrizia Frei et al., "Use of Mobile Phones and Risk of Brain Tumours: Update of Danish Cohort Study," BMJ, 20 Oct. 2011, https://www.cancer.dk/dyn/resources/File/file/9/1859/1385432841/1_bmj_2011_pdf.pdf.

[10] Jean Yang, Twitter post, 11 Sep. 2018, 1:49 am, https://twitter.com/jeanqasaur/status/1039435801736536064.

[11] Mike Masnick, "Thomas Goolnik Gets Google To Forget Our Story About Him Getting Google To Forget Stories About Thomas Goolnik," *Techdirt*, 9 Oct. 2018, https://www.techdirt.com/articles/20181003/23545140776/thomas-goolnik-gets-google-to-forget-our-story-about-him-getting-google-to-forget-stories-about-thomas-goolnik.shtml.

B. GDPR by the Numbers

Overly broad, prescriptive, and ambiguous privacy regulations come at the expense of prosperity and innovation. One need only look across the pond at the impact GDPR has had for the EU's struggling digital economy. Exhibit C details some of these statistics, which include hundreds of dollars in direct welfare losses for EU citizens; more than 1,100 U.S news websites no longer accessible on the continent; and a drop in independent digital ad prices of up to 40 percent. GDPR has been in effect for less than six months.

Exhibit C: GDPR Statistics

Number	Description
1,139	Number of U.S. news sites unavailable in the EU due to GDPR, as of November 2, 2018.[12]
$150 billion	Estimated total GDPR compliance costs for large U.S. firms.[13]
$296	Estimated direct welfare loss per European citizen due to increased prices from GDPR.[14]
25 to 40%	Estimated drop in prices on independent ad exchanges in Europe following GDPR.[15]
75,000	Estimated number of Data Protection Officers to be hired due to GDPR.[16]
$8.8 billion	Total damages claimed in four complaints filed against Google and Facebook within seven hours of GDPR going into effect.[17]
1,600	Number of Microsoft engineers working on GDPR-related compliance projects.[18]
42,230	Number of complaints that have been filed with the European Data Protection Board.[19]
4%	Share of global annual revenue that GDPR fines can impose on firms.[20]
220,000	Number of name tags that must be removed from buildings in Vienna to avoid up to $23 million in GDPR fines.[21]

[12] Joseph O'Connor, "Websites Not Available in the European Union after GDPR," accessed 2 Nov. 2018, https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr.

[13] Daniel Castro and Michael McLaughlin, "Why the GDPR Will Make Your Online Experience Worse," *Fortune*, 23 May 2018, http://fortune.com/2018/05/23/gdpr-compliant-privacy-facebook-google-analytics-policy-deadline/.

[14] Hosuk Lee-Makiyama, "The Political Economy of Data: EU Privacy Regulation and the International Redistribution of Its Costs." In *Protection of Information and the Right to Privacy-A New Equilibrium?*, Springer, Cham, 2014, pp. 85-94, https://link.springer.com/chapter/10.1007/978-3-319-05720-0_5.

[15] Jessica Davies, "'The Google Data Protection Regulation': GDPR Is Strafing Ad Sellers," *Digiday*, 4 June 2018, https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/.

[16] Rita Heimes and Sam Pfeifle, "Study: GDPR's Global Reach to Require at Least 75,000 DPOs Worldwide," International Association of Privacy Professionals, 9 Nov. 2016, https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/.

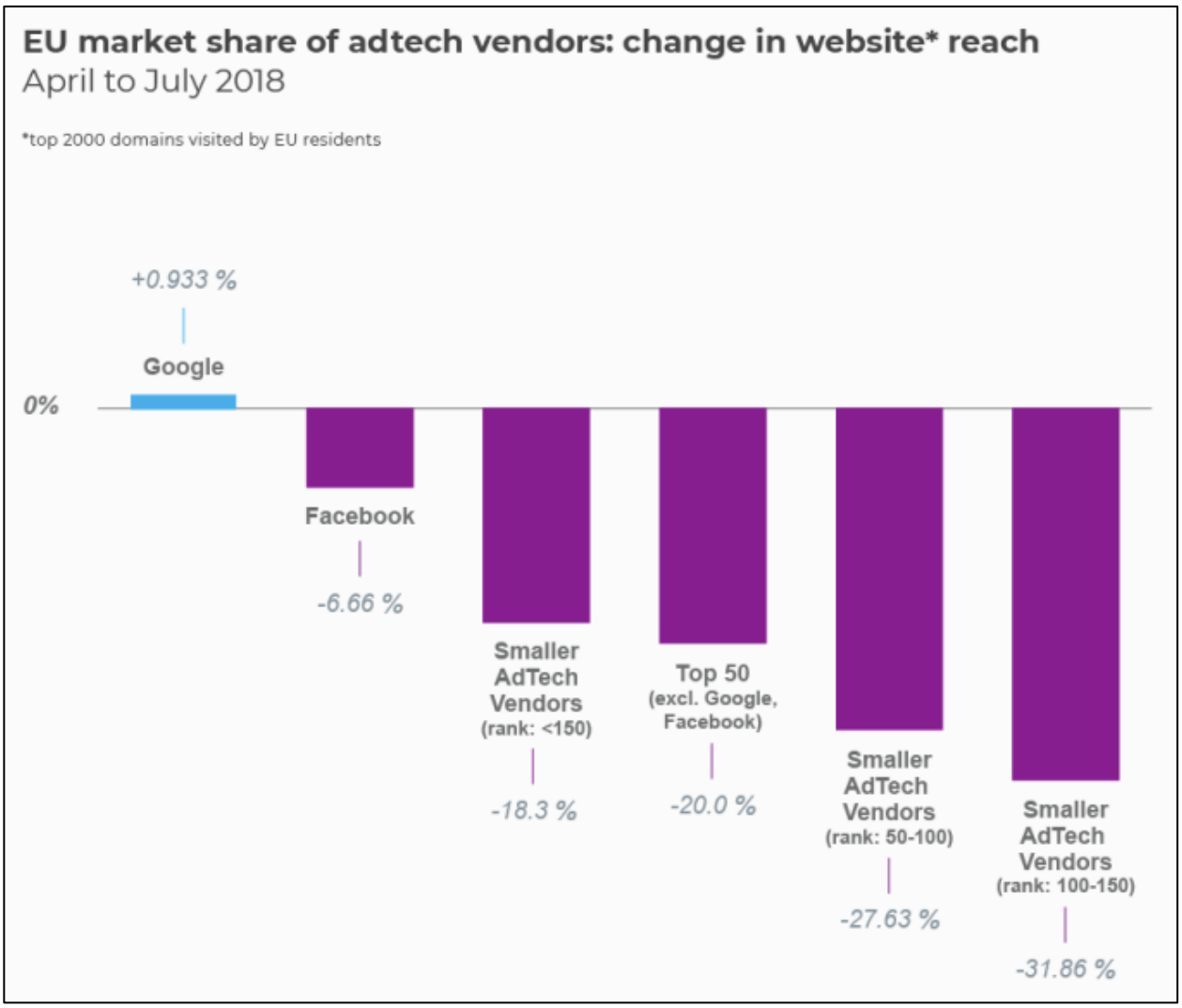
[17] "GDPR: *noyb.eu* Filed Four Complaints Over "Forced Consent" Against Google, Instagram, WhatsApp, and Facebook," noyb.eu, 25 May 2018, https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf.

[18] Julie Brill, "Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data," Microsoft On the Issues, 21 May 2018, https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/.

[19] Natasha Lomas, "Europe Is Drawing Fresh Battle Lines Around the Ethics of Big Data," *TechCrunch*, 3 Oct. 2018, https://techcrunch.com/2018/10/03/europe-is-drawing-fresh-battle-lines-around-the-ethics-of-big-data/.

[20] GDPR, Article 83.

Exhibit D: EU Adtech Vendors



It is tragically ironic that one branch of the EU is fining tech giants like Google billions of dollars for being too dominant in their markets, while at the same time another branch is passing regulations that further entrench the tech giants, creating the regulatory equivalent of a revolving door of fines for American technology companies. But the stakes for privacy regulation are much higher in the United States than they are in Europe. Privacy pragmatism has been a contributing factor in America's rise to global tech dominance. "Of the world's 15 largest digital firms, all are American or Chinese. Of the top 200, eight are European."[22] In the United States, the digital economy supports 5.9 million jobs and accounts for 6.5% of GDP.[23]

---

[21] Rick Noack, "Europe's Privacy Laws Are Now So Tough, They Are Taking Names Off Doorbells in Vienna," *The Washington Post*, 19 Oct. 2018, https://www.washingtonpost.com/world/2018/10/19/europes-privacy-laws-are-now-so-tough-they-are-taking-names-off-doorbells-vienna/?utm_term=.33498c77645a.

[22] "Europe's History Explains Why It Will Never Produce a Google," *The Economist*, 13 Oct. 2018, https://www.economist.com/europe/2018/10/13/europes-history-explains-why-it-will-never-produce-a-google.

[23] "Initial Estimates Show Digital Economy Accounted for 6.5 Percent of GDP in 2016," National Telecommunications and Information Administration, 15 Mar. 2018, https://www.ntia.doc.gov/blog/2018/initial-estimates-show-digital-economy-accounted-65-percent-gdp-2016.

Exhibit E: GDPR Graveyard

Company Name	Date announced	Category	Products/services affected
Brent Ozar Unlimited[24]	Dec 18, 2017	Other	IT consulting services
Drawbridge[25]	Mar 7, 2018	Marketing	Cross-device identity service
Verve[26]	Apr 18, 2018	Marketing	Mobile programmatic advertising
Gravity Interactive[27]	Apr 25, 2018	Video game	Ragnarok Online, Dragon Saga (MMORPGs)
Uber Entertainment[28]	Apr 26, 2018	Video game	Super Monday Night Combat
Tunngle[29]	Apr 29, 2018	Video game	VPN for playing LAN games online
CoinTouch[30]	May 3, 2018	Blockchain	Peer-to-peer cryptocurrency exchange
Streetlend[31]	May 3, 2018	Social	Tool-sharing platform for neighbors
Unroll.me[32]	May 5, 2018	Marketing	Inbox management app
Stool Root[33]	May 5, 2018	Security	Cybersecurity and IT services
Edge of Reality[34]	May 7, 2018	Video game	Loadout (free-to-play arena shooter game)

[24] Brent Ozar, "GDPR: Why We Stopped Selling Stuff to Europe," Brent Ozar Unlimited, 18 Dec. 2017, https://www.brentozar.com/archive/2017/12/gdpr-stopped-selling-stuff-europe/.
[25] James Hercher, "Drawbridge Exits Media Business In Europe Before GDPR Storms The Castle," *AdExchanger*, 7 Mar 2018, https://adexchanger.com/mobile/drawbridge-exits-media-business-europe-gdpr-storms-castle/.
[26] Ronan Shields, "Verve to Focus on US Growth as It Plans Closure of European Offices Ahead of GDPR," *The Drum*, 18 Apr. 2018, https://www.thedrum.com/news/2018/04/18/verve-focus-us-growth-it-plans-closure-european-offices-ahead-gdpr.
[27] Ivana Kottasová, "These Companies Are Getting Killed by GDPR," CNNMoney, 11 May 2018, https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html.
[28] Owen S. Good, "Super Monday Night Combat Will Close Down, Citing EU's New Digital Privacy Law," *Polygon*, 28 Apr. 2018, https://www.polygon.com/2018/4/28/17295498/super-monday-night-combat-shutting-down-gdpr.
[29] "GDPR: Tech Firms Struggle with EU's New Privacy Rules," *BBC*, 24 May 2018, https://www.bbc.com/news/technology-44239126.
[30] Priyeshu Garg, "European GDPR Fear: P2P Cryptocurrency Exchange CoinTouch Shuts Down," BTCMANAGER, 7 May 2018, https://btcmanager.com/european-gdpr-fear-p2p-cryptocurrency-exchange-cointouch-shuts-down/.
[31] David Bisson, "Lending Website Cites GDPR Concerns as Reason Why It Shut Down," *Tripwire*, 30 Apr. 2018, https://www.tripwire.com/state-of-security/latest-security-news/lending-website-cites-gdpr-concerns-as-reason-why-it-shut-down/.
[32] Natasha Lomas, "Unroll.me to Close to EU Users Saying It Can't Comply with GDPR," *TechCrunch*, 5 May 2018, https://techcrunch.com/2018/05/05/unroll-me-to-close-to-eu-users-saying-it-cant-comply-with-gdpr/.
[33] James Sanders, "To Save Thousands on GDPR Compliance, Some Companies Are Blocking All EU Users," *TechRepublic*, 7 May 2018, https://www.techrepublic.com/article/to-save-thousands-on-gdpr-compliance-some-companies-are-blocking-all-eu-users/.
[34] Alice O'Connor, "Loadout Shutting Down This Month Ahead of GDPR," *Rock, Paper, Shotgun*, 9 May 2018, https://www.rockpapershotgun.com/2018/05/09/loadout-shutting-down-because-of-gdpr/.

Lithium[35]	May 10, 2018	Social	Klout, a social reputation service
Seznam[36]	May 11, 2018	Social	Social network for students
IO Interactive[37]	May 11, 2018	Video game	Hitman: Absolution (stealth shooter game)
Monal[38]	May 17, 2018	Social	XMPP chat app
Parity[39]	May 18, 2018	Blockchain	KYC services for ICO's
Family Tree DNA[40]	May 18, 2018	Other	Ysearch, Mitosearch (public genetic-genealogy databases)
Twitter[41]	May 22, 2018	Social	Roku, Android TV, and Xbox apps discontinued
Payver[42]	May 24, 2018	Security	Dashcam app
Williams-Sonoma[43]	May 25, 2018	Other	Housewares retailer

The economic costs of privacy fundamentalism should not be underrated. Exhibit E provides an account of companies that have gone out of business, shut down a service, or left the European market altogether due to GDPR compliance costs. Furthermore, free public genealogy databases like GEDMatch are what made it possible to catch the Golden State Killer. Unfortunately, GDPR is causing some of them to shut down, which will make it harder to catch criminals in the future.[44]

PART II: RESOLVING THE PRIVACY PARADOX

B. The Department is also seeking feedback on the proposed high-level goals for an end-state for U.S. consumer-privacy protections.

1. **Are there other goals that should be included, or outcomes that should be expanded upon?**
2. **Are the descriptions clear? Beyond clarity, are there any issues raised by how the issues are described?**

---

[35] Shannon Liao, "Klout Is out and There's Nary a Pout," *The Verge*, 10 May 2018, https://www.theverge.com/tldr/2018/5/10/17340714/klout-lithium-social-media-reputation-tool-clout.

[36] Kottasová, *supra* note 31.

[37] "Hitman Absolution Service Message," IO Interactive, accessed on 8 Nov. 2018, https://www.ioi.dk/hitman-absolution-service-message/.

[38] "GDPR: Removing Monal from the EU," 17 May 2018, https://monal.im/blog/gdpr-removing-monal-from-the-eu/.

[39] "PICOPS to Be Discontinued on May 24th, 2018," Parity Technologies, 18 May 2018, https://www.parity.io/picops-discontinued-may-24th-2018/.

[40] Megan Molteni, "The Key to Cracking Cold Cases Might Be Genealogy Sites," *Wired*, 1 June 2018, https://www.wired.com/story/police-will-crack-a-lot-more-cold-cases-with-dna/.

[41] Todd Spangler, "Twitter Is Shutting Down Apps for Roku, Xbox and Android TV Devices," *Variety*, 22 May 2018, https://variety.com/2018/digital/news/twitter-roku-xbox-android-tv-gdpr-1202818827/.

[42] Hannah Kuchler, "US Small Businesses Drop EU Customers over New Data Rule," *The Financial Times*, 24 May 2018, https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04.

[43] Danica Kirka, "Amid Confusion, EU Data Privacy Law Goes into Effect," *The Associated* Press, 25 May 2018, https://apnews.com/3b6945f9f5794d87bb5c78bb093f724a.

[44] Molteni, *supra* note 44.

3. **Are there any risks that accompany the list of goals, or the general approach taken by the Department?**

G. Are there other ways to achieve U.S. leadership that are not included in this RFC, or any outcomes or high-level goals in this document that would be detrimental to achieving the goal of achieving U.S. leadership?

American leadership on privacy issues is best achieved by implementing a set of rules and regulations that provides the optimal balance between privacy and prosperity. To find this balance, policymakers first need to understand how Americans weigh these different values. For that, regulators need to understand the privacy paradox.

In surveys, people often say that they value online privacy highly. But people's actions imply they do not value it very much at all. So is this just another example of cheap talk? Once people need to bear the cost of privacy, do they choose to give it away? Revealed preferences via observed consumer behavior often tell us more than stated preferences for this reason. The literature on the economics of privacy is relatively clear on this issue.

Most research and behavioral studies conclude that privacy is highly context-dependent. Privacy valuations are subject to cognitive biases, including social desirability bias (e.g., people are less likely to share embarrassing information) and the endowment effect.[45] Most people care a great deal about privacy harms that result in material and financial costs, such as identity theft, or the revelation of sensitive personal information to their close social circles. They tend to care far less about data collected about their purchasing patterns and website browsing activity by companies storing that information on distant, largely-inaccessible data server farms. This is especially true when consumers receive what they judge to be considerable benefits at a functional cost to them of zero dollars and zero cents.

Privacy choices inevitably involve trade-offs — more privacy often means less convenience, fewer choices, and higher costs. A 2000 study by Sayre and Horne "examined actual disclosure and found consumers would freely trade personal information in exchange for small discounts at a grocery store. The widespread existence of retail and service loyalty programs indicates this practice covers many categories."[46] A 2017 paper from Athey, Catalini, and Tucker noted that:

> *Whenever privacy requires additional effort or comes at the cost of a less smooth user experience, participants are quick to abandon technology that would offer them greater protection. This suggests that privacy policy and regulation has to be careful about regulations that inadvertently lead consumers to be faced with additional effort or a less smooth experience in order to make a privacy-protective choice.*[47]

---

[45] Tiffany Barnett White, "Consumer Disclosure and Disclosure Avoidance: A Motivational Framework," *Journal of Consumer Psychology*, Vol. 14, No. 1 & 2: 41-51 (2004), https://www.researchgate.net/profile/Tiffany_White2/publication/279703855_Consumer_Disclosure_and_Disclosure_Avoidance_A_Motivational_Framework/links/593966d2458515320611460 6/Consumer-Disclosure-and-Disclosure-Avoidance-A-Motivational-Framework.pdf.

[46] Patricia A. Norberg, et al. "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors." *Journal of Consumer Affairs*, Vol. 41, No. 1: 100-126 (2007).

[47] Susan Athey, et al., *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*. No. w23488. National Bureau of Economic Research, 2017, https://www.ftc.gov/system/files/documents/public_comments/2017/09/00010-141392.pdf.

A. Prevent a Patchwork by Preempting State-Level Privacy Laws

One of the most important goals of any federal baseline privacy law should be creating regulatory harmony between the fifty states. As Jennifer Huddleston Skees, a research fellow at the Mercatus Center at George Mason University, points out, coherent digital privacy rules demand a federal approach:

> *The Internet by its very nature transcends states borders and any state laws aimed at impacting privacy are likely to have national and global impact. This is not what is intended by federalism and not just the case for states like California with a significant amount of tech companies. If there are 50 different state laws than [sic] new online intermediaries will have [to] develop 50 different compliance policies or the most restrictive state will become the de facto standard for everyone left in the industry. As Jeff Kosseff points out, a world of 50 variations of the same privacy law based on users would … likely require significant changes to [out-of-state content creators'] existing systems and place an undue burden on content creators and users.*[48]

B. The FTC Needs Reinforcements

The FTC has brought more than 500 enforcement actions on privacy- and security-related issues since 1998.[49] The Commission is clearly policing the beat. But with only 57 full-time staff working on these cases, it needs more help to fulfill its statutory mandate. The FTC remains the appropriate federal agency to enforce consumer privacy (with exceptions for sectoral privacy laws outside the FTC's jurisdiction, such as HIPAA). It is important to take steps to ensure that the FTC has the necessary resources and direction to enforce consumer privacy laws in a manner that balances the need for strong consumer protections, legal clarity for organizations, and the flexibility to innovate.

What the agency does not need, however, is broader statutory authority to effectuate its mission. Any federal framework for privacy governance should not include providing the FTC with formal rulemaking authority. The FTC's existing grant of statutory authority under Section 5 — which provides the agency the power to police "unfair and deceptive" practices — is already broad enough to cover the entire universe of conceivable privacy-related harms.

PART III: SUMMARY OF RECOMMENDATIONS

1. **Maintain sector-based privacy regulation for sensitive healthcare, education, and financial information;**
2. **Preempt state regulation of online privacy by passing baseline federal privacy regulations that are predictable, minimalist, consistent and simple;**
3. **Baseline privacy regulation should aim to ensure transparency, security, risk management, and accountability, but not at the cost of limiting innovation;**

---

[48] Jennifer Huddleston Skees, "The Problem of Patchwork Privacy," *The Technology Liberation Front*, 15 Aug. 2018, https://techliberation.com/2018/08/15/the-problem-of-patchwork-privacy/.

[49] Maureen K. Ohlhausen, "Putting the FTC Cop Back on the Beat," Remarks at the Future of Internet Freedom, 28 Nov. 2017, https://www.ftc.gov/system/files/documents/public_statements/1280393/putting_the_ftc_cop_back_on_the_beat_mko.pdf.

4. **Generally speaking, a broad ethos of accountability for any organization that collects data should be prefered over more prescriptive or precautionary mandates; and**

5. **Examine the potential need to allocate additional resources for the FTC."**

CONCLUSION

The United States should continue on the path of privacy pragmatism that has enabled the explosive growth of the domestic digital economy and made America the envy of entrepreneurs and innovators around the world. Otherwise, we run the risk of losing that mantle of preeminence to the emerging Chinese technology sector and joining the Europeans in a race to the bottom economically.

We would like to thank the NTIA for the opportunity to comment on these issues and look forward to continued engagement on these and other topics.