NEW AMERICA

June 2021

Does Data Privacy Need its Own Agency?

Comparing FTC and DPA Enforcement of a Future Federal Privacy Law

Christine Bannan & Raj Gambhir

About the Author(s)

Christine Bannan is policy counsel at New America's Open Technology Institute, focusing on platform accountability and privacy.

Raj Gambhir was a Legal/Public Policy intern with New America's Open Technology Institute, working with the platform accountability and privacy teams.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Open Technology Institute

OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Contents

Introduction

There is general consensus among members of the U.S. Congress, industry, civil society, and the public that the United States needs federal privacy legislation, but there is no consensus on how such legislation would be enforced and by whom.[1] While the seemingly constant barrage of consumer data breaches and pervasive tracking across the internet have numbed the public and led to a sense of "privacy nihilism," two major scandals in 2017 and 2018 managed to grab the public's attention and cause Congress to consider policy solutions. Credit bureau Equifax announced in September 2017 that it exposed the personal information of 143 million (later revealed to be 147 million) people.[2] Then, in March 2018, journalists broke the story that Facebook's data practices enabled the harvesting of 50 million (later revealed to be 87 million) users' personal data, which was sold to political analytics firm Cambridge Analytica.[3] Congress held a series of hearings on both incidents and introduced various privacy and data security bills, but ultimately did not pass legislation. The Federal Trade Commission (FTC), however, brought enforcement actions in response to both events and reached settlements with the companies.

The FTC worked with the Consumer Financial Protection Bureau (CFPB) and state attorneys general to reach a settlement with Equifax that created a fund to offer affected consumers a cash payment of $125 or free credit monitoring.[4] However, the fund was capped at $300 million,[5] and high demand for cash payments led the FTC to encourage consumers to accept the free credit monitoring option.[6] If every affected person filed a claim, the payout would only be 21 cents. So Equifax added an additional hurdle requiring that people had credit monitoring services before the breach to obtain the cash award.[7] The demand for cash payments should have come as no surprise, given that the breach affected half the U.S. population and consumers were unlikely to trust the company that breached their personal information to protect them from identity theft.

The FTC also reached consent orders with both Facebook and Cambridge Analytica, levying a record-breaking $5 billion fine against Facebook.[8] However, senators called the fine a "far cry from the type of monetary figure that would alter the incentives and behavior of Facebook and its peers."[9] New America's Open Technology Institute (OTI) commented that Facebook "was rewarded on the stock market for the settlement, the settlement imposed no meaningful restrictions on Facebook's data collection and sharing practices, and structural changes require a tenacious overseer to ensure compliance or they may lead to nothing."[10] Facebook was already under a consent order with the FTC when the Cambridge Analytica event occurred, and yet the third-party assessors responsible for monitoring compliance did not report it. The new consent order

contained several changes to Facebook's privacy practices, but the past failures of the FTC's compliance system call its efficacy into question.

These two incidents helped Congress recognize that the privacy status quo is not working for consumers—but is it just because the United States lacks adequate privacy laws, or is the FTC also to blame? If Congress passes comprehensive privacy legislation, should the FTC be tasked with enforcing it? Or should Congress create a new agency?

OTI hosted an event and wrote a report in 2019 that explored different mechanisms of enforcement: federal agency (whether FTC or a new agency), state attorneys general and state legislation, and a private right of action empowering individuals to sue.[11] This report builds on that work to compare the relative merits of FTC enforcement versus enforcement by a new agency. Data privacy has become an issue of national economic, political, and social significance over the past few decades. The implementation of the European General Data Protection Regulation (GDPR) in 2018,[12] the California Consumer Privacy Act (CCPA) in 2020,[13] and the passage of the Virginia Consumer Data Protection Act in 2021[14] have heightened political impetus to implement a comprehensive federal privacy law. Moreover, the California Privacy Rights Act, [15] an extensive amendment to CCPA, established a new agency—the California Privacy Protection Agency—to enforce the CCPA/CPRA rather than relying on attorney general enforcement.[16]

Discussions regarding enforcement of proposed federal privacy laws prior to late 2019 tended to focus on the question of whether or not enforcement should be shared between the FTC and state attorneys general. A lengthy Congressional Research Service (CRS) report on data privacy laws from March 2019 only addresses the possibility of creating a new agency to enforce federal privacy laws in one footnote.[17] However, growing recognition of the weak enforcement of the GDPR in the first three years of its existence has heightened the importance of enforcement mechanisms in U.S. privacy legislation.[18]

This report explores the question of whether comprehensive federal data privacy legislation should be enforced by the FTC or a new agency created by Congress. This report will use the acronym "DPA" to refer to the general concept of a new agency to enforce federal privacy law in the United States. In Europe, this acronym refers to Data Protection Authorities that enforce the GDPR—in this report, those will be referred to as European DPAs.[19] In the U.S. context, the acronym DPA covers the different agency titles—Data Privacy Agency, Digital Privacy Agency, Data Protection Agency, and Data Protection Authority—that appear in various bills and proposals. To avoid confusion, this report will discuss particular DPA proposals in reference to their authorizing legislation.

A number of lawmakers, members of civil society, and privacy experts have called for the creation of a dedicated regulatory body to enforce federal privacy

law. In 2019, Representatives Anna Eshoo (D-CA) and Zoe Lofgren (D-CA) introduced the Online Privacy Act of 2019, which would create a DPA.[20] In 2020, senators also introduced two additional federal privacy bills that would establish DPAs: Senator Sherrod Brown's (D-OH) Data Accountability and Transparency Act,[21] and Senator Kirsten Gillibrand's (D-NY) Data Protection Act.[22] This report will compare these three bills to one another and to FTC enforcement. We will also draw comparisons between the DPA proposals and two relatively new federal agencies: the CFPB and the Privacy and Civil Liberties Oversight Board (PCLOB). This report will not cover proposals like the Digital Platform Agency proposed by former FCC Chairman Tom Wheeler[23] and Public Knowledge's Harold Feld,[24] which are sector-specific agencies that would have jurisdiction much broader than privacy.

Comprehensive privacy legislation will only have a substantive effect on business practices if there is a federal agency with the will, ability, and resources to enforce the law rigorously. We do not conclude that a new agency or an enhanced FTC is inherently a better enforcement agency. Rather, we argue that Congress should assess the effectiveness of proposals for either type of enforcement model using key metrics: authority, independence, resistance to regulatory capture, effectiveness of enforcement, budget, and feasibility.

This report first explains the differences between proposals that empower the FTC and proposals that create a DPA to enforce privacy legislation. It then explains the similarities and differences between the DPAs proposed by the Eshoo-Lofgren, Gillibrand, and Brown bills. The final section of the report defines each metric, explains why it is important for Congress to consider, and evaluates how an empowered FTC and DPA would compare along the metrics.

Editorial disclosure: This report discusses policies by Facebook and Google, both of which are funders of work at New America but did not contribute funds directly to the research or writing of this piece. New America is guided by the principles of full transparency, independence, and accessibility in all its activities and partnerships. New America does not engage in research or educational activities directed or influenced in any way by financial supporters. View our full list of donors at ***www.newamerica.org/our-funding****.*

Revamped FTC or New Agency

To provide context into our analysis of whether data privacy should be regulated by the FTC or a new agency, we will first detail the current shortcomings of FTC regulation of data privacy along with proposals to address these limitations in authority and resources. Next, we will explain why a growing number of lawmakers and members of civil society are calling for the establishment of a new agency that would be narrowly focused on enforcing federal privacy law. Finally, we will briefly outline the three bills put forward by lawmakers.

Isn't the FTC Already the U.S. Privacy Agency?

Federal privacy law in the United States consists of many distinct statutes that regulate data practices in different industries rather than a comprehensive or "omnibus" approach. While Congress has delegated enforcement authority for several specific privacy statutes to the FTC, that has never included general privacy authority. Under this sectoral approach to privacy, the enforcement of privacy statutes is delegated to different federal agencies based on subject matter. For example, the Health Insurance Portability and Accountability Act (HIPAA) is enforced by the U.S. Department of Health and Human Services,[25] the Family Educational Rights and Privacy Act is enforced by the U.S. Department of Education,[26] and the Telephone Consumer Protection Act is enforced by the Federal Communications Commission (FCC).[27]

Congress has assigned the FTC enforcement responsibility for the Children's Online Privacy Protection Act (COPPA),[28] the Fair Credit Reporting Act,[29] the Fair and Accurate Credit Transactions Act,[30] the Gramm-Leach-Bliley Act,[31] the Identity Theft Assumption and Deterrence Act,[32] the Telemarketing and Consumer Fraud and Abuse Prevention Act,[33] and the Controlling the Assault of Non-Solicited Pornography and Marketing Act.[34] These statutes comprise only a small fraction of the 82 statutes enforced by the FTC.[35]

The FTC is an enforcement agency with the dual mission to protect consumers and promote competition in the American economy.[36] The agency has three bureaus: the Bureau of Competition, the Bureau of Consumer Protection, and the Bureau of Economics.[37] The Division of Privacy and Identity Protection is one of eight divisions within the Bureau of Consumer Protection.[38] Despite privacy comprising such a small component of the FTC's organizational structure, the agency has been treated as the de facto privacy authority in the United States.

The Federal Trade Commission Act of 1914 gave the FTC authority to stop "unfair or deceptive acts or practices in or affecting commerce" (UDAP),[39] and the commission applies this authority to privacy and data security where a sector-

specific privacy statute is inapplicable. The FTC applies UDAP authority to questions of data privacy not covered by specific statute because the United States does not have a designated general privacy authority.[40] What constitutes an "unfair or deceptive" activity with regard to data processing has been decided on a case-by-case basis over many years in a process that scholars have labelled a "Common Law of Privacy."[41] With a privacy law in place, a regulator would be able to refer to a set of codified data privacy standards rather than rely primarily on a common law approach.

It is the norm among industrialized countries to have independent regulators for privacy and data protection and omnibus—rather than sectoral—privacy laws. The United States is the only country in the Organisation for Economic Co-operation and Development (OECD) without a DPA.[42] The Global Privacy Assembly began in 1979 and convenes 130 privacy and data protection authorities from around the world.[43] The FTC represents the United States at these convenings, even though the United States is one of the few countries without a dedicated privacy agency.[44] European countries have had DPAs since a 1995 EU directive.[45]

The FTC fulfills some of the roles that foreign privacy authorities do, including collaborating with European DPAs on enforcement matters.[46] However, the FTC cannot be considered America's privacy regulator because there are several other U.S. agencies that enforce various privacy statutes. In the absence of comprehensive privacy legislation, the United States does not have an omnibus privacy law to enforce.[47] The FTC's existing role as the closest approximation to a U.S. privacy regulator has led many lawmakers drafting federal comprehensive privacy legislation to propose delegating enforcement authority to the FTC.[48] Competing proposals to delegate enforcement of privacy legislation to a new DPA have challenged the assumption that the FTC should enforce an omnibus privacy law. This report seeks to evaluate the strengths and weaknesses of different enforcement agency approaches.

Expanding FTC Enforcement

Stakeholders that advocate for FTC enforcement agree that the agency would need additional authority and resources if Congress decides to delegate enforcement authority of new privacy legislation to the FTC.[49] Broadly speaking, these concerns stem from constraints on the agency's rulemaking authority and resources along with a perception that the FTC has too many competing priorities within its broad mandate to focus sufficiently on regulating data privacy.[50] After a brief discussion of these concerns, we will outline the various solutions to these shortcomings proposed by lawmakers and members of civil society.

Privacy advocates argue that current restraints on FTC rulemaking would limit effective enforcement of a future comprehensive privacy law unless Congress explicitly takes steps to address these obstacles. Rulemaking is the process by which government agencies draft and implement regulations in order to fulfill their mandate and implement laws passed by Congress.[51] Normally, agencies engage in rulemaking in accordance with the standards set forth by the Administrative Procedures Act (APA).[52] However, with a few exceptions, the FTC must adhere to stricter standards for rulemaking under the Magnuson-Moss Warranty Act.[53]

Congress passed Magnuson-Moss specifically to make rulemaking more burdensome for the agency after a series of FTC rules in the 1970s were perceived by some to be an overextension of the commission's mandate, particularly the attempted ban on advertising directed at children.[54] The Magnuson-Moss procedures include about 20 additional procedures and analysis requirements not found in the APA.[55]

FTC rulemaking under this stricter standard takes, on average, six-times longer than rulemaking done under the APA standard.[56] Under APA procedures, the FTC was able to issue rules in 2.94 years on average. Since Magnuson-Moss was passed, it takes the agency 5.57 years on average.[57] Congress has granted APA rulemaking powers to the FTC pursuant to the enforcement of certain statutes, but the commission lacks the ability to utilize the APA standard when dealing with matters of consumer protection that fall outside of these statutes. That is why the FTC is in the peculiar position of being able to utilize APA rulemaking to oversee the privacy of individuals below the age of 13 under COPPA but cannot do the same for adults.[58] Congress allowed the FTC to use APA rulemaking 12 times between 1993 and 2009, and the agency was able to issue rules in 287.25 days on average under this typical rulemaking process.[59]

In a future privacy law, this limitation could easily be addressed by specifying that FTC rulemaking pursuant to the new law would be done under APA rather than Magnuson-Moss standards. FTC Commissioner Christine S. Wilson has advocated for the inclusion of such a provision in any future privacy legislation.[60] Proposed privacy bills from both Republicans and Democrats—such as Senator Roger Wicker's (R-MS) proposal[61] and Senator Maria Cantwell's (D-WA) proposal [62]—would provide the FTC at least some form of APA rulemaking powers to enforce a new privacy law.

The FTC's small size and limited resources have also contributed to the agency's weak privacy enforcement record. As of April 2019, the agency had only about 40 full-time employees overseeing data privacy.[63] That's only about one-third the size of the Irish Data Protection Commission, the lead European authority responsible for supervising Google and Facebook, which is responsible for

bringing more cases than any other European DPA. The FTC's budget and personnel will be discussed in more depth later in the report.

If Congress passes privacy legislation that assigns enforcement authority to the FTC, it could increase the agency's budget to hire more staff and create a fourth bureau in addition to the agency's Bureau of Competition, Bureau of Consumer Protection, and Bureau of Economics.[64] Proponents of creating a Bureau of Technology within the FTC, such as former Commissioner Terrell McSweeny, argue that organizing the work the commission does on technology within its own bureau will enable the FTC to better attract the personnel needed to enforce relevant data privacy laws.[65] Senator Ron Wyden's (D-OR) Mind Your Own Business Act of 2019 would add 125 new staff to existing bureaus and 50 staff to a new Bureau of Technology.[66] The FTC could also create a new bureau without legislation if it obtained approval from the Congressional Appropriations Committees.[67]

Creating a New DPA

Members of Congress have introduced three bills that would establish a new agency to enforce comprehensive federal privacy legislation. These proposals reflect a concern that simply allocating more resources to the FTC or expanding its rulemaking power would not necessarily equip the agency to sufficiently protect user privacy rights. Some argue that the FTC lacks the "digital DNA" to regulate the distinctive digital economy.[68] Others point to the FTC's lackluster track record on regulating digital platforms as reason to create a new agency.[69]

DPA proposals call for the creation of a dedicated agency to enforce federal data privacy law. Much of DPA discourse draws from foreign data privacy enforcement models. The Eshoo-Lofgren DPA, in many ways, draws from the EU's GDPR. In addition to including many of the GDPR's privacy rights, the Eshoo-Lofgren DPA proposal—and, indeed, most DPA proposals—are modeled after the EU's Data Protection Authorities, the entities tasked with enforcing the GDPR.[70] Under the European model, the DPA investigates breaches of privacy laws and, if applicable, levies fines.[71] In addition to this investigative and punitive function, the DPA consults with industry and civil society to promote compliance and refine the enforcement of federal privacy law.[72]

A Closer Look at the Eshoo-Lofgren, Gillibrand, and Brown DPA Proposals

We will close the background section of the report by delineating the key differences between the Eshoo-Lofgren, Gillibrand, and Brown DPA bills so as to ground our subsequent analysis of the strengths and weaknesses of FTC versus DPA enforcement.

	Eshoo-Lofgren's "Digital Privacy Agency" (DPA)	Gillibrand's "Data Protection Agency" (DPA)	Brown's "Data Accountability and Transparency Agency" (DATA)
Agency Mandate	To enforce the privacy rights and responsibilities enumerated in this Act, including the right to access, correct, and delete data collected by entities processing data. (§ 101-109, 201-215) To convene advisory boards to represent different stakeholders' interests (§ 306-308). To create a grant program for the development of open source machine learning training data sets. (§ 311)	To enforce privacy statutes and rules, investigate, subject to rulemaking (§ 6), and bring civil actions against entities conducting data related UDAP (§ 9), and directly supervise very large covered entities. (§ 8)	To enforce the privacy rights and responsibilities enumerated in this Act (§ 101-105, 201-208); supervise covered entities for compliance with requirements (§ 309); and issue regulations. (§ 308)
Covered Entities	A person who intentionally collects, processes, or maintains personal information and sends or receives such personal information over the internet or a similar communications network. Excludes natural persons engaged in de minimis collection or processing activity. (§ 2)	Any person that collects, processes, or otherwise obtains personal data with the exception of an individual processing personal data in the course of personal or household activity. (§ 3)	Any person that collects, uses, or shares personal data. Excludes de minimis amounts of data and data solely for personal reasons. The term "data aggregator" is used rather than "covered entity." (§ 3)
Leadership Structure	Director, appointed by President, serving 5-year term and subject to cause removal.* (§ 301)	Director, appointed by President, serving 5-year term and subject to cause removal.* (§ 4)	Director, appointed by President, serving 5-year term and subject to cause removal.* (§ 301)
Rulemaking Authority	Yes, pursuant to the purposes and objectives of the Act (which is also comprehensive privacy legislation). (§ 302)	Yes, pursuant to enforcement of federal privacy legislation (not part of this Act) and the Act itself. (§ 7)	Yes, pursuant to enforcement of federal privacy law and the Act itself. Must consider the impact of proposed rules and consult with civil society groups and members of the public. (§ 308)
Relationship to FTC	The FTC and the DPA will negotiate an agreement for coordinating enforcement actions. (§ 405)	FTC authority under existing privacy law to issue rules, guidelines, and reports ceded to the new agency. (§ 12)	The DATA will coordinate with the FTC to promote consistent regulatory treatment of personal data. (§ 304)
Private Right of Action	Yes, a person who is harmed by a violation of this Act may bring an action for injunctive relief and damages either independently or through nonprofit collective representation. (§ 407)	No, consumers may submit complaints to the DPA, and the agency will respond with follow-up actions. No action may be brought under this Act more than 3 years after the date of discovery of the alleged violation. (§ 9)	Yes, any person may bring an action against violators of this Act, including the DATA itself, filed within 5 years of the date of discovery of the alleged violation. (§ 401)
Civil Penalties	May not exceed the product of the maximum penalty stipulated for UDAP in FTC Act and the number of individuals affected by the violation. (§ 408)	Three tiers: $5,000 daily fine for violation of agency order, $25,000 daily fine for reckless violation of federal privacy law, and $1,000,000 daily fine for each knowing violation of federal privacy law. (§ 9)	DATA may fine data aggregators whose gross revenues exceed $25 million or annually use the data of 50,000 or more individuals. The Director may determine the fine amount. (§ 306)
Preemption of State Law	No preemption language, meaning that state law is not preempted. (Source)	Preempts state laws that provide less protection than what is provided by the Act itself. (§ 10)	Preempts state laws that provide less protection than what is provided by the Act itself. (§ 602)
Relationship to Comprehensive Federal Privacy Law	Bill is a comprehensive privacy framework. Mandate of the proposed DPA would be to enforce the privacy rights and requirements in the bill. (§ 1)	Bill is not a comprehensive privacy framework. Mandate of the proposed DPA would be to ensure the full application of existing and future federal privacy law. (§ 6)	Bill is a comprehensive privacy framework. Mandate of the proposed DATA would be to protect individuals from violations of federal privacy law and to ensure that federal privacy law, including this Act, is enforced consistently. (§ 307)

NEW AMERICA

**These bills were introduced before Seila Law v. Consumer Financial Protection Bureau held this leadership structure unconstitutional.*

**These bills were introduced before Seila Law v. Consumer Financial Protection Bureau held this leadership structure unconstitutional.*

These three bills use an agency structure led by a single director with a five-year term who can only be removed for cause. This directorship structure is identical to the CFPB, the financial regulator established by the Dodd-Frank Act in the wake of the 2008 financial crisis.[73] However, in June 2020, the Supreme Court ruled in *Seila Law v. Consumer Financial Protection Bureau* that the CFPB leadership structure is unconstitutional: a single director must be removable at will rather than only for cause.[74] In contrast to the single-director model, the FTC is headed by a five-person commission where no more than three members can be from the same party.[75] The significance of *Seila Law v. Consumer Financial Protection Bureau* will be discussed in more depth in the "Independence" section below.

The three bills propose DPAs with differing levels of power. The Eshoo-Lofgren DPA has the narrowest mandate, while the Brown DPA has the broadest. The primary function of the Eshoo-Lofgren DPA is to enforce comprehensive privacy law. In practice, this would mean applying fines to entities that process data in such a way that is prohibited by their bill. The Brown DPA would broadly also fine violators of the bill's framework, and would directly supervise large data processing entities.

In the following section, we will compare the Digital Privacy Agency model as outlined in the Eshoo-Lofgren privacy proposal with FTC enforcement of a comprehensive privacy law along six relevant metrics.

Comparing the FTC and DPA

The privacy bills that delegate enforcement to the FTC and those that create a new agency are quite different in form, so it is helpful to compare the two options by their likely effectiveness. Taking a holistic view of agency performance, we will assess the options along six metrics: statutory authority, independence, resistance to regulatory capture, effectiveness of enforcement, budget, and feasibility. To make these comparisons, we will largely rely on past agency performance in the case of the FTC, and analogous agencies in the case of the proposed DPA. These analogous agencies are the CFPB and the various European DPAs.

Statutory Authority

In this section, statutory authority refers to an agency's ability, as granted by a statute, to enforce a privacy law. This analysis will focus primarily on rulemaking authority. First, we will detail the current limitations of FTC statutory authority. Then, we will explore how new comprehensive federal privacy legislation could expand FTC statutory authority. Finally, we will compare this model of an empowered FTC to a model of a new DPA.

Legislation could empower either the FTC or a new agency to enforce a new statute specifically for data privacy. The relevant comparison is then between a new agency and an FTC empowered with expanded rulemaking authority by a comprehensive privacy law*, not* the current FTC limited to Section 5 authority. Therefore, it is not accurate to point to "the limitations of its generic statute" as proof that the FTC is not up to the task of regulating the digital economy,[76] because all proposals analyzed in this report that designate the FTC as the agency responsible for enforcement give the agency specific statutory authority in addition to their Section 5 authority. Indeed, Congress has already granted the agency the power to regulate specific domains of privacy, such as children's online privacy, in addition to and separate from its Section 5 authority.

Currently, the FTC's general data privacy regulation authority is based in its statutory authority under Section 5 of the FTC Act, which tasks the FTC with regulating "unfair or deceptive acts or practices."[77] The FTC has applied its Section 5 consumer protection authority to privacy and security and developed a body of decisions that operate like common law.[78] The FTC's approach primarily relies on corporate self-regulation under the notice and consent model, bringing enforcement actions against companies that have *deceptively* violated their own privacy policies and public representations made to users about how they protect their privacy and security.[79] While this strategy has led to a number of enforcement actions over the years,[80] the notice and consent model relies on a

number of faulty assumptions, including the notion that the average user *can* meaningfully consent to privacy policies.[81] Section 5 enforcement actions relating to data privacy have largely been based on the deceptiveness standard. Since the 2015 Wyndham case, the FTC also brings actions against firms that *unfairly* open their users' data to security risks.[82]

Proponents of FTC enforcement of a future federal privacy law assert that the agency's history of Section 5 enforcement constitutes a rich body of accumulated common law forged through "complaints, consent decrees, and various reports" that provides a sound and flexible basis to enforce a comprehensive privacy law.[83] The answer to how the FTC's privacy enforcement under Section 5 would interact with comprehensive privacy legislation is ambiguous because bills designating the FTC as the enforcing authority have taken divergent approaches. The Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA Act) would prevent the FTC from utilizing its UDAP authority in matters relating to data privacy or security in a manner inconsistent with the act.[84] Contrastingly, the Consumer Online Privacy Rights Act (COPRA) would treat violations of the act as a UDAP under Section 5.[85]

In order to make a fair comparison between an empowered FTC and a DPA, we will review the FTC's enforcement record of COPPA, the Children's Online Privacy Protection Act of 1998.[86] COPPA is a federal privacy law that gives the FTC APA rulemaking authority to enforce the act.[87] Under COPPA, the FTC has promulgated rules every ten years as mandated by Congress: once in 2000 to implement the 1998 law, and again in 2013 to expand the definition of personally identifiable information (PII) to better reflect the increasing importance of cookies and geolocational data in surveilling young children.[88] In 2019, the FTC opened a comment period to consider a new set of amendments to the COPPA rules, which may encourage general audience platforms to identify child-directed third-party content and ensure it complies with COPPA.[89]

The FTC has brought almost 30 cases under COPPA. In 2019, the commission issued its two largest COPPA fines of $5.7 million and $170 million to ByteDance and YouTube, respectively.[90] While the FTC lauded the outcome of the YouTube settlement,[91] many considered the settlement ineffective. COPPA's original sponsor, Senator Ed Markey (D-MA), claimed that the settlement lacked a deterrent value and did not provide sufficient structural injunctions because it would not prevent future violations.[92] Advocacy groups have also criticized the FTC's enforcement of COPPA, arguing that the agency has failed to rigorously enforce the policy.[93]

One example of this insufficient enforcement is the FTC's failure to investigate Facebook for violations of COPPA. In February 2019, over a dozen advocacy organizations filed a complaint against Facebook[94] accusing the company of violating COPPA by knowingly tricking children into making in-game purchases.[95]

The commission has not followed up on this complaint. In fact, Facebook has never been fined under COPPA, despite multiple high-profile revelations that the company likely violated the law.[96] At this time, it is unclear whether the FTC would effectively utilize the APA rulemaking authority granted to it by a future federal privacy law.

Budget and Personnel

Generally, proposals for a U.S. DPA are modeled on the CFPB and the European DPAs.[97] Therefore, this section's analysis will make comparisons to the budget and personnel of the CFPB and European authorities when appropriate. The most detailed DPA proposal is the Eshoo-Lofgren proposal. This bill allocates a $550 million yearly budget to the new agency, which would use those funds to hire about 1,600 employees.[98] This budget seems to be proportional to the number of staff being hired. The CFPB, a comparable agency to the Eshoo-Lofgren DPA, had budget for FY 2019 of approximately $510 million and used those funds to employ 1,465 full-time staff.[99]

The legislative proposals that do not establish a new agency do not increase FTC staff and budget at levels comparable to the DPA proposals. In FY 2019, the most recent year for which budget and full-time employee data is available, the FTC budget amounted to $311 million with 1,101 full-time staff.[100] As of 2020, only about 40 of those employees were doing privacy enforcement work.[101]

Proposals delegating privacy law enforcement to the FTC generally bolster an existing bureau or establish a new bureau within the agency. Senator Wyden's Mind Your Own Business Act of 2019 would create a new 50-person Bureau of Technology within the FTC and add 125 employees to the Bureau of Consumer Protection—100 of whom would do privacy enforcement work.[102] This would bring the total number of FTC employees doing privacy enforcement work up to about 190. While the Wyden bill does not provide figures for how much adding 175 new employees would cost, former FTC Chairman Joseph Simons estimated that a $50 million budget increase from Congress would enable the FTC to hire 160 new staff.[103] Under this proposal, the number of employees working on privacy would more than triple. However, it would still only be about one-tenth the size of the Eshoo-Lofgren DPA proposal.

Most pertinent to this analysis is the sheer personnel and budget disparity between a hypothetical DPA and an empowered FTC. As mentioned before, the Eshoo-Lofgren proposal gives the agency a yearly budget of $550 million and about 1,600 full time employees.[104] By contrast, the FTC currently has a budget of $311 million and 1,101 employees.[105] The Wyden proposal would boost the agency budget by about $55 million and lead to the hiring of 175 additional staff.[106] In total, that would boost the commission's budget to about $366 million and

bring the number of staff up to 1,276. Those staff would have to add the enforcement of a federal privacy bill to a long list of existing responsibilities, including Section 9 antitrust investigations, merger review, international investigations, Section 5 enforcement, and many more.[107] In contrast, the Eshoo-Lofgren DPA would largely be tasked with enforcing the federal privacy law and consulting with users, academia, and small businesses.

A further consideration beyond the structure of the DPA is the risk that a hostile administration or Congress could starve the agency of funds. The CFPB faced this issue under former President Donald Trump's administration, when Mick Mulvaney became the director of the agency and asked staff to cut the budget by 20 percent.[108] Even in Europe, where DPAs have faced funding challenges, each of the European DPAs has funding and personnel levels dramatically higher than the FTC's Division of Privacy and Identity Protection.[109] However, data privacy has historically been a bipartisan issue and is not likely to be as politically controversial as the CFPB.

Whether Congress decides to empower the FTC or create a new agency as the enforcer of privacy legislation, it will need to appropriate a larger budget and more personnel in order for enforcement to be meaningful.

Independence

Agency independence depends on the extent to which the executive branch can direct the work of the agency.[110] While there is no one specific feature of independence common to all independent executive agencies, there are agency design choices that make an agency more independent or less independent.[111] A central determinant of agency independence is the extent to which the president can remove the leadership personnel: at will, meaning for any reason, or for cause, meaning only for "inefficiency, neglect of duty, or malfeasance in office."[112]

Two Supreme Court cases challenging the independence of the FTC and CFPB have made it clear that there are two constitutionally permissible administrative agency models: either an agency is led by a single director serving at the will and direction of the president or an agency is led by a multi-member body that can only be removed for cause. The 1935 case *Humphrey's Executor v. United States* held that the FTC structure was constitutional because "Congress could create expert agencies led by a *group* of principal officers removable by the President only for good cause."[113] The 2020 case *Seila Law v. Consumer Financial Protection Bureau* held that the CFPB structure was unconstitutional because an *independent* administrative agency cannot be led by a single director, therefore any agency with a single director must be removable at will by the president.[114]

In response to this decision, the CFPB will continue to be led by a single director, but that director will now be removable by the president for any reason, thereby limiting the agency's independence. By contrast, the FTC is considered an independent administrative agency because it is led by a five-member Commission with statutory removal protections that insulate commissioners from the president's direction.

All three DPA bills are based on the original leadership model of the CFPB and therefore must be modified to pass constitutional muster. The bill sponsors can decide to strike the for-cause removal requirements: § 301(c)(3) in Eshoo-Lofgren, § 4(c)(3) in Gillibrand, and § 301(c)(3) in Brown. Alternatively, they could revise their bills to adopt a multi-member body similar to the FTC. However, this seems unlikely because DPA advocates seek to differentiate their proposed agencies from the FTC, and a single director model is a significant point of distinction.

There are benefits to both the independence of the FTC and the single-director DPA model. Many federal agencies are led by a single director rather than a commission, including the administrator of the Environmental Protection Agency and the attorney general of the Department of Justice (DOJ). The tradeoff to their relative efficiency is less stability. The 2018 Sourcebook of United States Executive Agencies published by the Administrative Conference of the United States endorses the multi-member commission structure as the most stable. The Conference stated, "Among the most durable agencies," meaning those least susceptible to elimination by hostile administrations, "are those multi-member bodies located outside the executive departments with features such as party-balancing limitations and fixed terms."[115]

A single-director DPA model is more likely to experience dramatic swings in policy dependent on the president in office, while the FTC model tends to be more consistent across administrations. The CFPB underwent extreme changes in policy under the Obama and Trump administrations that some attribute to the single-director structure.[116] Some scholars argue, however, that single-director agencies are much more efficient than the alternative and that these ideological swings are simply the result of directors reflecting the partisan inclinations of whichever president they were appointed by.[117] Moreover, data privacy legislation has more bipartisan support than Dodd-Frank did when it was passed and therefore would likely not be as susceptible to the dramatic partisan shifts as the CFPB.

The FTC's multi-member structure requires three commissioners to vote for any significant agency action. The agency is often criticized by consumer advocates for failing to act forcefully to curtail industry abuses, and this weakness can at least be partially attributed to its multi-member structure. As Ralph Nader put it in a letter to the commissioners in 2019, "With slight surges over the past fifty years since our FTC report, The Nader Report on the Federal Trade Commission,

was published in 1969, followed by some reforms, the FTC remains a largely moribund, sluggish, frightened, alleged watchdog for the American consumer."[118] A single director can act more swiftly and decisively, whereas building consensus is inherently slower and typically requires compromise that tempers the desired outcome of the most progressive commissioner. In fact, this is part of the Supreme Court's rationale behind the *Seila Law* decision: an agency led by a single director wields more power than an agency led by a multi-member body and therefore must be more accountable to the president.

However, the Commission's multi-member structure leaves a record of dissent that agencies led by single directors lack. Contentious decisions in the FTC are usually accompanied by at least one dissenting statement because of the multi-member commission structure and party balancing requirements. As time passes and market conditions change, these dissents can be vital in informing legislative and regulatory action. To give a prominent example, in 2007, Pamela Jones Harbour was the only FTC commissioner to dissent from the FTC's decision to allow Google's acquisition of DoubleClick.[119] Harbour emphasized that the decision would not only lead to anticompetitive outcomes but would also degrade the data privacy of Google users.[120] With Google currently under scrutiny for its acquisition of Fitbit[121] and facing a DOJ antitrust suit,[122] Harbour's dissent has found new relevancy. In 2020, Harbour's dissent was invoked by academics,[123] DOJ staff,[124] and FTC commissioners.[125]

In short, the multi-member commission structure allows the agency and other interested bodies to have a public paper trail for controversial decisions and draw on those documents if circumstances change. However, privacy advocates, academics, and other experts also oppose agency decisions they view as harmful to privacy, serving essentially the same function as commissioner dissents. Therefore, while the dissents of commissioners are valuable, other stakeholders would be able to fulfill that role in an agency under a single director.

If Congress decides to delegate enforcement of new privacy legislation to the FTC, the multi-member body structure would provide continued stability. However, this structure may exacerbate the agency's record of perceived insufficient enforcement that was the impetus for the sponsors of the three DPA bills to prefer a new agency. The single-director DPA model can provide more agility and nimbleness but will not have independence from the president. Members of Congress will view the tradeoff between efficiency and independence differently, leading them to prefer one leadership structure over the other.

Resistance to Regulatory Capture

Regulatory capture refers to conditions where an agency is ineffective because it is so heavily influenced by the entities it regulates.[126] If the enforcer of a future

comprehensive privacy law is (or becomes) captured by the tech industry, the law will not have the intended result of improving privacy protections. Conventional wisdom holds that agencies with broad mandates are less prone to regulatory capture than sector-specific agencies because they are "more likely to resist pressure from any one interest group."[127] This argument assumes that a DPA would be more likely to be captured than the FTC. However, the reality is more complex because a DPA differs from the typical sector-specific regulator.

Sector-specific regulators solely regulate certain industries and develop specialized expertise due to their focus.[128] The FCC and CFPB, for example, regulate the telecommunications industry and the consumer finance industry, respectively. The FTC differs from this model. It has a broad mandate to "protect consumers and promote competition" across the economy.[129] The FCC is often seen as being more susceptible to industry influence than the FTC: a 2015 report from the Edmond J. Safra Center for Ethics found that the FCC suffers from extensive regulatory capture from the telecommunications industry.[130] However, while the FTC may not be as prone to regulatory capture as other agencies, it is not immune. Capture can occur through personnel changes: 63 percent of top FTC officials "have revolving door conflicts of interest involving work on behalf of the technology sector."[131]

While the three proposed DPAs all have much narrower mandates than the FTC, they are not typical sector-specific agencies because they are technically industry neutral. The DPAs would have an outsized regulatory impact on companies like Google, Amazon, Facebook, and Apple, but their scope would not be limited to digital platforms. Rather, they would regulate the data practices of companies across various industries. For example, the Eshoo-Lofgren bill defines a covered entity as any non-natural person who "intentionally collects, processes, or maintains personal information; and sends or receives such personal information over the internet or a similar communications network."[132] These three DPAs differ from Digital Platform Agency proposals that define jurisdiction based on the type of entity, defining "digital platform" as the covered sector.[133] While the focus of the DPAs would likely be on digital platforms initially, as different sectors of the economy rely more on data-intensive practices, this focus could shift and expand over time to other sectors. Therefore, a DPA should not be assumed to fall prey to the same level of regulatory capture that sector-specific regulators often experience.

Effectiveness of Enforcement

Effectiveness of enforcement is the capacity of a regulatory agency to enforce the statutes and regulations it is responsible for in a manner that deters future violations. While it is difficult to assess the enforcement effectiveness of a

hypothetical empowered FTC and a DPA, we can look to analogous cases to bolster our analysis.

As proponents of a DPA have noted, the FTC has not effectively followed through with its own enforcement actions.[134] The effectiveness of enforcement is difficult to define and measure because it is affected by many different variables. Even if the FTC were to receive additional funding and personnel, the commission's mandate is so broad that there is a significant risk that it would not be able to regulate data privacy as effectively as a new agency with a single mission. Congress has already tasked the FTC with the enforcement of more than 70 laws, eight of which can be categorized as privacy and data security laws.[135] The FTC would need to make an effort to prioritize privacy over other consumer protection issues, otherwise privacy legislation could just become another statute to add to the agency's list. Moreover, Congress has constrained FTC authority multiple times in history, and it is possible that the commission's authority could be constrained again in the future.[136]

Perhaps the best example to illustrate the FTC's inadequate enforcement is the agency's lackluster response to Facebook's breach of its 2011 consent decree with the FTC. While the FTC has been lauded for fining Facebook a historic $5 billion in 2019 for violating the decree, there is ample evidence that the commission could have punished the company for violations much sooner, possibly preventing the Cambridge Analytica scandal.[137] The 2019 fine only represented a month of Facebook's revenue and the company's stock *rose* in the aftermath of the announcement.[138] That the Cambridge Analytica scandal occurred while Facebook was under an FTC consent decree throws further doubt on the commission's ability to effectively enforce data privacy regulations and ultimately protect internet users in a timely way.

As discussed in the budget and personnel section, the Eshoo-Lofgren DPA would have a staff of about 1,600. Due to the sector specific focus of this DPA, it could focus on hiring staff with deep knowledge and expertise in the digital economy and data privacy. The staff and budget size would give the DPA the expertise, personnel, and resources to effectively respond to consumer complaints regarding tech companies, actively enforce the laws it would be tasked with, and consult with relevant stakeholders (such as civil society, industry, or users) regarding the best allocation of its resources.

Feasibility

Feasibility in this section means the logistical ease of operations. It is relatively more feasible for Congress to empower the FTC with additional funding and rulemaking authority to enforce a federal privacy law than it is to have Congress create a new agency for this purpose.

On a basic level, empowering the FTC is more feasible than standing up a new agency because of path dependency. The FTC would be better positioned than other existing agencies to become the U.S.'s official data privacy agency because it already enforces some sectoral privacy statutes and brings enforcement actions under its general consumer protection authority, and regularly hosts bilateral discussions on data privacy and security with data protection authorities from around the world.[139] While the FTC has not always effectively utilized its authority, the FTC's accumulated experience places it in a position to become the enforcer of a comprehensive privacy legislation more quickly than a DPA.

If Congress did establish a DPA through legislation, it would need to overcome substantial barriers to stand up a new independent agency. The case of the PCLOB—the Privacy and Civil Liberties Oversight Board—is instructive. Congress established the PCLOB as an independent agency in 2007 to review counterterrorism activities to ensure that they include adequate safeguards for privacy and civil liberties.[140] However, the agency did not actually come into existence until 2012 when the Senate confirmed its first four board members.[141] This five-year period delayed the agency's ability to fulfill its mission and serve the public.

After authorization of the entity and confirmation of leadership, a new independent agency will face basic hurdles to set up agency infrastructure and operations that can be mitigated through agency design. A new agency needs office space; internet, email, and phone service; and a complete complement of staff including not only subject matter experts but also everything from human resources to internal information technology specialists. At a prior OTI panel, David Medine, who served as the first chairman of the PCLOB and also previously served as special counsel at the CFPB, argued that a new agency should "sit on the structure of the old agency until it's ready to separate."[142] Medine noted that unlike with the PCLOB, the CFPB staff benefited from being able to use Treasury Department payroll, email, and website infrastructure before the agency was ready to stand on its own. The Brown DPA is the only DPA proposal to use this model of operating on the Federal Reserve System infrastructure.[143] Therefore, while it is more feasible for an existing agency to begin its enforcement duties, a DPA could avoid initial operational problems that other new agencies have faced if it utilized an existing agency's infrastructure.

Conclusion

In this report, we have endeavored to use six metrics—authority, independence, resistance to regulatory capture, effectiveness of enforcement, budget, and feasibility—to assess proposals for an expanded FTC or a new DPA to enforce a new federal privacy law. As these proposals are refined and new ones are introduced, we should continue to use these criteria to measure the strengths and weaknesses of each option. Neither the FTC nor a new DPA is inherently a better option across all of the metrics we have identified. Moreover, members of Congress can take steps to design solutions to optimize a proposal's performance on each of these standards.

Given the importance of digital privacy to civil rights,[144] commerce,[145] and self-determination,[146] the question of which agency will enforce a national privacy regime cannot and should not be taken lightly. As Congress considers the various comprehensive privacy bills, members should consider the different factors that affect optimal agency design for the enforcement of a federal privacy law.

Notes

1 Sam Sabin, "States Are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritize Protection of Online Data," Morning Consult, April 27, 2021, https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/

2 "Equifax Announces Cybersecurity Incident Involving Consumer Information," Equifax, September 7, 2017, https://investor.equifax.com/news-and-events/press-releases/2017/09-07-2017-213000628

3 Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach," *Guardian*, March 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

4 "Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach," Federal Trade Commission, July 22, 2019, https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related

5 Alfred Ng and Steven Musil, "Equifax data breach may affect nearly half the US population," CNET, September 7, 2017, https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population/

6 Robert Schoshinski, "Equifax data breach: Pick free credit monitoring," Federal Trade Commission, July 31, 2019, https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-pick-free-credit-monitoring

7 Charlie Warzel, "Equifax Doesn't Want You to Get Your $125. Here's What You Can Do." *New York Times*, September 16, 2019, https://www.nytimes.com/2019/09/16/opinion/equifax-settlement.html

8 "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," Federal Trade Commission, July 24, 2019, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions ; "FTC Grants Final Approval to Settlement with Former Cambridge Analytica CEO, App Developer over Allegations they Deceived Consumers over Collection of Facebook Data," Federal Trade Commission, December 18, 2019, https://www.ftc.gov/news-events/press-releases/2019/12/ftc-grants-final-approval-settlement-former-cambridge-analytica

9 Senators Markey, Blumenthal, and Hawley Demand Answers from FTC over Reported Facebook Settlement, July 16, 2019, https://www.markey.senate.gov/news/press-releases/senators-markey-blumenthal-and-hawley-demand-answers-from-ftc-over-reported-facebook-settlement

10 "FTC Announces Historic, Yet Insufficient, Settlement with Facebook for Privacy Violations," press release, Open Technology Institute, July 24, 2019, https://www.newamerica.org/oti/press-releases/ftc-announces-historic-yet-insufficient-settlement-facebook-privacy-violations/

11 Becky Chao, Eric Null, and Claire Park, "Enforcing a New Privacy Law: Who Should Hold Companies Accountable?," Open Technology Institute, November 20, 2019, https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/

12 "General Data Protection Regulation: GDPR," Intersoft Consulting, June 3, 2017, https://gdpr-info.eu/

13 "California Consumer Privacy Act (CCPA)," Xavier Becerra: Attorney General, August 14, 2020, https://oag.ca.gov/privacy/ccpa

14 Rebecca Klar, "Virginia governor signs comprehensive data privacy law," The Hill, March 2, 2021, https://thehill.com/policy/technology/541290-

virginia-governor-signs-comprehensive-data-privacy-law

15 "The California Privacy Rights Act of 2020," IAPP, February 5, 2021, https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/

16 "California Officials Announce California Privacy Protection Agency Board Appointments," Office of Governor: Gavin Newsom, March 17, 2021, https://www.gov.ca.gov/2021/03/17/california-officials-announce-california-privacy-protection-agency-board-appointments/

17 "Data Protection Law: An Overview," Congressional Research Service, March 25, 2019, https://fas.org/sgp/crs/misc/R45631.pdf

18 "GDPR: Three years in, and its future and success are still up in the air," AccessNow, May 25, 2021, https://www.accessnow.org/gdpr-three-years/

19 "What are Data Protection Authorities (DPAs)?," European Commission, June 22, 2018, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

20 "H.R.4978 - Online Privacy Act of 2019," Congress.gov, December 18, 2019, https://www.congress.gov/bill/116th-congress/house-bill/4978/text

21 "Data Accountability and Transparency Act of 2020," United States Senate Committee on Banking, Housing, and Urban Affairs, June 18, 2020, www.banking.senate.gov/imo/media/doc/Brown%20-%20DATA%202020%20Discussion%20Draft.pdf

22 "S.3300 - Data Protection Act of 2020," Congress.gov, February 13, 2020, https://www.congress.gov/bill/116th-congress/senate-bill/3300

23 Tom Wheeler, Phil Verveer, and Gene Kimmelman, "New Digital Realities; New Oversight Solutions," Shorenstein Center on Media, Politics and Public Policy, August 20, 2020, https://shorensteincenter.org/new-digital-realities-tom-wheeler-phil-verveer-gene-kimmelman/

24 Harold Feld, "The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms," Roosevelt Institute and Public Knowledge, May 8, 2019, https://www.publicknowledge.org/assets/uploads/documents/Case_for_the_Digital_Platform_Act_Harold_Feld_2019.pdf

25 "Health Information Privacy," HHS.gov, September 8, 2015, https://www.hhs.gov/hipaa/index.html

26 "Family Educational Rights and Privacy Act (FERPA)," U.S. Department of Education, September 11, 2003, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

27 "FCC Actions on Robocalls, Telemarketing," Federal Communications Commission, February 26, 2016, https://www.fcc.gov/general/telemarketing-and-robocalls

28 "Children's Online Privacy Protection Act," Federal Trade Commission, March 6, 2015, https://www.ftc.gov/enforcement/statutes/childrens-online-privacy-protection-act

29 "Fair Credit Reporting Act," Federal Trade Commission, January 18, 2014, https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act

30 "Fair and Accurate Credit Transactions Act of 2003," Federal Trade Commission, February 11, 2015, https://www.ftc.gov/enforcement/statutes/fair-accurate-credit-transactions-act-2003

31 "Gramm-Leach-Bliley Act," Federal Trade Commission, September 12, 2015, https://

www.ftc.gov/enforcement/statutes/gramm-leach-bliley-act

32 "Identity Theft Assumption and Deterrence Act of 1998," Federal Trade Commission, September 10, 2015, https://www.ftc.gov/enforcement/statutes/identity-theft-assumption-deterrence-act-1998

33 "Telemarketing and Consumer Fraud and Abuse Prevention Act," Federal Trade Commission, September 21, 2015, https://www.ftc.gov/enforcement/statutes/telemarketing-consumer-fraud-abuse-prevention-act

34 "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)," Federal Trade Commission, March 3, 2015, https://www.ftc.gov/enforcement/statutes/controlling-assault-non-solicited-pornography-marketing-act-2003-can-spam-act

35 "Statutes Enforced or Administered by the Commission," Federal Trade Commission, December 8, 2013, https://www.ftc.gov/enforcement/statutes

36 "What We Do," Federal Trade Commission, December 8, 2013, https://www.ftc.gov/about-ftc/what-we-do

37 "Bureaus & Offices," Federal Trade Commission, December 8, 2013, https://www.ftc.gov/about-ftc/bureaus-offices

38 "Our Divisions," Federal Trade Commission, December 11, 2013, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions

39 "A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority," Federal Trade Commission, December 8, 2013, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority

40 "Facebook's $5 Billion Privacy Settlement with the Federal Trade Commission," Federal Trade Commission, August 8, 2019, https://fas.org/sgp/crs/misc/LSB10338.pdf

41 Daniel J. Solove and Woodrow Hartzog, "The FTC and the New Common Law of Privacy," Columbia Law Review, February 14, 2017, https://cyberlaw.stanford.edu/files/publication/files/SSRN-id2312913.pdf

42 "The U.S. Urgently Needs a Data Protection Agency," Electronic Privacy Information Center, February 13, 2020, https://epic.org/dpa/

43 "Global Privacy Assembly," Global Privacy Assembly, December 25, 2019, https://globalprivacyassembly.org/

44 "List of Accredited Members," Global Privacy Assembly, December 25, 2019, https://globalprivacyassembly.org/participation-in-the-assembly/list-of-accredited-members/

45 European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,Chap. VI Art 28.4, October 24, 1995.

46 "Privacy & Data Security: Update: 2019," Federal Trade Commission, March 6, 2020, https://ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf

47 "The U.S. Urgently Needs a Data Protection Agency," Electronic Privacy Information Center, February 13, 2020, https://epic.org/dpa/

48 "Data Protection Law: An Overview," Congressional Research Service, March 25, 2019, https://fas.org/sgp/crs/misc/R45631.pdf

49 "Statement of Michelle Richardson, Director, Privacy & Data Center for Democracy & Technology before the United States Senate Committee on the

Judiciary GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation," Center for Democracy & Technology, March 12, 2019, https://www.judiciary.senate.gov/imo/media/doc/Richardson%20Testimony1.pdf

50 Becky Chao, Eric Null, and Claire Park, "The FTC is Currently the Primary Privacy Enforcer but its Authority is Limited," Open Technology Institute, November 20, 2019, https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/the-ftc-is-currently-the-primary-privacy-enforcer-but-its-authority-is-limited

51 "A Guide to the Rulemaking Process," Office of the Federal Register, January 2011, https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf

52 "Data Protection Law: An Overview," Congressional Research Service, March 25, 2019, https://fas.org/sgp/crs/misc/R45631.pdf

53 "Magnuson Moss Warranty-Federal Trade Commission Improvements Act," Federal Trade Commission, https://www.ftc.gov/enforcement/statutes/magnuson-moss-warranty-federal-trade-commission-improvements-act

54 Cameron F. Kerry and Daniel J. Weitzner, "Rulemaking and its discontents: Moving from principle to practice in federal privacy legislation," Brookings Institution, June 5, 2019, https://www.brookings.edu/blog/techtank/2019/06/05/rulemaking-and-its-discontents-moving-from-principle-to-practice-in-federal-privacy-legislation/

55 Jeffrey S. Lubbers, "It's Time to Remove the 'Mossified' Procedures for FTC Rulemaking," The George Washington Law Review, 1979, www.gwlr.org/wp-content/uploads/2016/01/83-Geo-Wash-L-Rev-1979.pdf

56 Id.

57 Jeffrey S. Lubbers, "Please Spare Us the Return of "Formal" Rulemaking," Yale Journal on Regulation, Notice and Comment, December 16, 2019, https://www.yalejreg.com/nc/please-spare-us-the-return-of-formal-rulemaking-by-jeffrey-s-lubbers/

58 "FTC's Use of Its Authorities to Protect Consumer Privacy and Security," Federal Trade Commission, June 23, 2020, https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf

59 Lubbers, "Please Spare Us the Return of "Formal" Rulemaking," https://www.yalejreg.com/nc/please-spare-us-the-return-of-formal-rulemaking-by-jeffrey-s-lubbers/

60 "A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation," Federal Trade Commission, February 6, 2020, www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf

61 "United States Consumer Data Privacy Act of 2019," Hunton Williams, March 2, 2020, www.privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/Nc7.pdf

62 "Consumer Online Privacy Rights Act," Congress.gov, December 3, 2019, https://www.congress.gov/116/bills/s2968/BILLS-116s2968is.pdf

63 "FTC Report on Resources Used and Needed for Protecting Consumer Privacy and Security," Federal Trade Commission, June 23, 2020, https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportresourcesprivacydatasecurity.pdf

64 "Bureaus & Offices," Federal Trade Commission, December 8, 2013, https://www.ftc.gov/about-ftc/bureaus-offices

65 "Facebook After Cambridge Analytica: What Should We Do Now?," Open Technology Institute, April 5, 2018, https://www.newamerica.org/oti/events/facebook-after-cambridge-analytica-what-should-we-do-now/

66 "Mind Your Own Business Act of 2019," Congress.gov, October 17, 2019, www.congress.gov/116/bills/s2637/BILLS-116s2637is.pdf

67 Jessica Rich, "Five reforms the FTC can undertake now to strengthen the agency," Brookings Institution, March 1, 2021, https://www.brookings.edu/blog/techtank/2021/03/01/five-reforms-the-ftc-can-undertake-now-to-strengthen-the-agency/

68 Tom Wheeler, Phil Verveer, and Gene Kimmelman, "The need for regulation of big tech beyond antitrust," Brookings Institution, September 23, 2020, www.brookings.edu/blog/techtank/2020/09/23/the-need-for-regulation-of-big-tech-beyond-antitrust/

69 Brian Barrett, "Fines Alone Aren't Enough to Slow Down Big Tech," *Wired*, September 4, 2019, www.wired.com/story/youtube-ftc-fines-alone-arent-enough/

70 Mike Masnick, "The Race Is On To Create A Federal Online Privacy Law: First Entry From Reps. Eshoo & Lofgren," TechDirt, November 7, 2019, https://www.techdirt.com/articles/20191105/12151543329/race-is-to-create-federal-online-privacy-law-first-entry-reps-eshoo-lofgren.shtml

71 "Data Protection Authorities," TermsFeed, January 18, 2021, www.termsfeed.com/blog/data-protection-authorities/#Powers_Of_Data_Protection_Authorities

72 "H.R.4978 - Online Privacy Act of 2019," Congress.gov, December 18, 2019, https://www.congress.gov/bill/116th-congress/house-bill/4978/text

73 "Building the CFPB," Consumer Financial Protection Bureau, July 18, 2011, https://www.consumerfinance.gov/data-research/research-reports/building-the-cfpb

74 Seila Law v. Consumer Financial Protection Bureau, 140 S. Ct. 2183 (2020), https://casetext.com/case/seila-law-llc-v-consumer-financial-protection-bureau

75 "Commissioners," Federal Trade Commission, December 30, 2013, https://www.ftc.gov/about-ftc/commissioners

76 "The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms," Roosevelt Institute and Public Knowledge, May 8, 2019, https://www.publicknowledge.org/assets/uploads/documents/Case_for_the_Digital_Platform_Act_Harold_Feld_2019.pdf

77 "Privacy and Security Enforcement," Federal Trade Commission, September 28, 2018, www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement

78 "The FTC and the New Common Law of Privacy," Columbia Law Review, February 14, 2017, https://cyberlaw.stanford.edu/files/publication/files/SSRN-id2312913.pdf

79 "The Scope and Potential of FTC Data Protection," The George Washington Law Review, January 12, 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2461096

80 "Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices," IAPP, October 2014, https://

iapp.org/media/pdf/resource_center/FTC-WhitePaper_V4.pdf

81 Claire Park, "How "Notice and Consent" Fails to Protect Our Privacy," Open Technology Institute, March 23, 2020, https://newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/

82 "FTC v. Wyndham Worldwide Corp.," Harvard Law Review, February 10, 2016, https://harvardlawreview.org/2016/02/ftc-v-wyndham-worldwide-corp/

83 "The FTC and the New Common Law of Privacy," Columbia Law Review, February 14, 2017, https://cyberlaw.stanford.edu/files/publication/files/SSRN-id2312913.pdf

84 "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act," Congress.gov, September 17, 2020, https://www.congress.gov/116/bills/s4626/BILLS-116s4626is.pdf

85 "Consumer Online Privacy Rights Act," Congress.gov, December 3, 2019, https://www.congress.gov/116/bills/s2968/BILLS-116s2968is.pdf

86 "Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. § 6501,et seq.," Office of the Law Revision Counsel: United States Code, April 21, 2000, https://uscode.house.gov/view.xhtml;jsessionid=23677D1360509C8C4C7DFC3107926347?req=granuleid%3AUSC-prelim-title15-chapter91&saved=%7CKHRpdGxlOjE1IHNlY3Rpb246NjUwMSBlZGl0aW9uOnByZWxpbSkgT1lgKGdyYW51bGVpZDpVU0MtcHJlbGltLXRpdGxlMTUtc2VjdGlvbjY1MDEp%7CdHJlZXNvcnQ%3D%7C%7C0%7Cfalse%7Cprelim&edition=prelim

87 "Children's Online Privacy Protection Rule ("COPPA")," Federal Trade Commission, December 12, 2013, https://ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

88 "Revised Children's Online Privacy Protection Rule Goes Into Effect Today," Federal Trade Commission, July 1, 2013, https://ftc.gov/news-events/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect

89 "FTC Seeks Comments on Children's Online Privacy Protection Act Rule," Federal Trade Commission, July 25, 2019, https://ftc.gov/news-events/press-releases/2019/07/ftc-seeks-comments-childrens-online-privacy-protection-act-rule

90 "Privacy & Data Security: Update: 2019," Federal Trade Commission, March 6, 2020, https://ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf

91 "FTC Press Conference on Settlement With Google / YouTube," Federal Trade Commission, September 4, 2019, https://www.ftc.gov/news-events/audio-video/video/ftc-press-conference-settlement-google-youtube

92 "COPPA Letter to FTC," Ed Markey: United States Senator for Massachusetts, October 4, 2019, https://www.markey.senate.gov/imo/media/doc/COPPA%20Letter%20to%20FTC%202019.pdf

93 "Don't Let Big Tech Gut COPPA," CCFC, October 17, 2019, https://commercialfreechildhood.org/dont-let-big-tech-gut-coppa/

94 "Over a Dozen Children's and Consumer Advocacy Organizations Request Federal Trade Commission to Investigate Facebook for Deceptive Practices," Common Sense Media, February 21, 2019, https://www.commonsensemedia.org/about-us/news/press-releases/over-a-dozen-childrens-and-consumer-advocacy-organizations-request

95 Nathan Halverson, "Facebook knowingly duped game-playing kids and their parents out of money,"

Reveal, January 24, 2019, https://www.revealnews.org/article/facebook-knowingly-duped-game-playing-kids-and-their-parents-out-of-money/

96 Harper Neidig, "Senators press Facebook over its handling of children's privacy," The Hill, August 6, 2019, https://thehill.com/policy/technology/456391-senators-raise-more-questions-about-facebook-handling-of-childrens-privacy

97 "Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016," EUR-Lex, Apr. 27, 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj

98 "H.R.4978 - Online Privacy Act of 2019," Congress.gov, December 18, 2019, https://www.congress.gov/bill/116th-congress/house-bill/4978/text

99 "Fiscal Year 2020: Annual performance plan and report, and budget overview," Bureau of Consumer Financial Protection, February 6, 2020, https://files.consumerfinance.gov/f/documents/cfpb_performance-plan-and-report_fy20.pdf

100 "FTC Appropriation and Full-Time Equivalent (FTE) History," Federal Trade Commission, March 11, 2019, https://ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation

101 "FTC Report on Resources Used and Needed for Protecting Consumer Privacy and Security," Federal Trade Commission, June 23, 2020, https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportresourcesprivacydatasecurity.pdf

102 "Mind Your Own Business Act," Congress.gov, October 17, 2019, https://congress.gov/116/bills/s2637/BILLS-116s2637is.pdf

103 "HHRG-116-IF17-20190508-SD010," Congress.gov, April 1, 2019, https://congress.gov/116/meeting/house/109415/documents/HHRG-116-IF17-20190508-SD010.pdf

104 "H.R.4978 - Online Privacy Act of 2019," Congress.gov, December 18, 2019, https://www.congress.gov/bill/116th-congress/house-bill/4978/text

105 "FTC Appropriation and Full-Time Equivalent (FTE) History," Federal Trade Commission, March 23, 2021, https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation

106 "Mind Your Own Business Act," Congress.gov, October 17, 2019, https://congress.gov/116/bills/s2637/BILLS-116s2637is.pdf

107 "A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority," Federal Trade Commission, October 2019, https://ftc.gov/about-ftc/what-we-do/enforcement-authority

108 "CFPB Acting Chief Asks Staff to Cut Budget by 20%," *Wall Street Journal*, June 12, 2018, https://wsj.com/articles/cfpb-acting-chief-asks-staff-to-cut-budget-by-20-1528842446

109 "Europe's governments are failing the GDPR," Brave, April 27, 2020, https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf

110 Milad Emamian et al.,"Debating Independent Agencies," Regulatory Review, January 25, 2020, https://www.theregreview.org/2020/01/25/saturday-seminar-debating-independent-agencies/

111 Kirti Datla and Richard L. Revesz, "Deconstructing Independent Agencies (and Executive Agencies)," Cornell Law Review, May 2013, https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=3270&context=clr

112 Amy Howe, "Opinion analysis: Court strikes down restrictions on removal of CFPB director but leaves bureau in place," SCOTUSblog, June 29, 2020, https://www.scotusblog.com/2020/06/opinion-analysis-court-strikes-down-restrictions-on-removal-of-cfpb-director-but-leaves-bureau-in-place/

113 Humphrey's Executor v. United States, 295 U.S. 602, 55 S.Ct. 869, (1935).

114 Seila Law v. Consumer Financial Protection Bureau, 140 S. Ct. 2183 (2020), https://casetext.com/case/seila-law-llc-v-consumer-financial-protection-bureau

115 "Sourcebook of United States Executive Agencies (Second Edition)," Administrative Conference of the United States, December 20, 2018, https://www.acus.gov/research-projects/sourcebook-united-states-executive-agencies-second-edition

116 Brian Knight, "From Chaos to a Commission: The consumer protection bureau's director debacle highlights its flawed structure," *U.S. News & World Report*, November 28, 2017, https://www.usnews.com/opinion/economic-intelligence/articles/2017-12-04/cfpb-chaos-shows-why-it-needs-a-bipartisan-commission-not-a-sole-director

117 Ganish Sitaraman and Ariel Dobkin, "The Choice Between Single Director Agencies and Multimember Commissions," Administrative Law Review, February 10, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3482162

118 Ralph Nader, letter to the FTC, July 17, 2019, https://www.corporatecrimereporter.com/wp-content/uploads/2019/07/ftc.pdf

119 "Dissenting Statement of Commissioner Pamela Jones Harbour," Federal Trade Commission, December 20, 2007, https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf

120 "Dissenting Statement of Commissioner Pamela Jones Harbour," Federal Trade Commission, December 20, 2007, https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf

121 "Google-Fitbit merger deal poses test for competition officials eyeing data giants," *Mint*, February 10, 2020,https://www.livemint.com/technology/tech-news/google-fitbit-merger-poses-test-for-competition-officials-eyeing-data-giants-11581332790062.html

122 "Justice Department Sues Monopolist Google For Violating Antitrust Laws," U.S. Department of Justice, Oct. 20, 2020, https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws

123 "Merger Breakups," Wisconsin Law Review, December 12, 2020, https://www.law.nyu.edu/sites/default/files/Menesh%20Patel.pdf

124 "Testimony of Sally Hubbard," Senate Judiciary Committee, March 10, 2020, https://www.judiciary.senate.gov/imo/media/doc/Hubbard%20Testimony.pdf

125 "Should We Block This Merger? Some Thoughts on Converging Antitrust and Privacy," Federal Trade Commission, January 30, 2020, https://www.ftc.gov/system/files/documents/public_statements/1565039/phillips_-_stanford_speech_10-30-20.pdf

126 Scott Hempling, "Regulatory Capture: Sources and Solutions," Emory Corporate Governance and Accountability Review, March 18, 2015, https://law.emory.edu/ecgar/content/volume-1/issue-1/essays/regulatory-capture.html

127 Rachel E. Barkow "Insulating Agencies: Avoiding Capture Through Institutional Design," Texas Law Review, January 2, 2011, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717037

128 "Independent Sector Regulators - Note by the United States," Organization for Economic Co-operation and Development, December 2, 2019, https://www.ftc.gov/system/files/attachments/us-submissions-oecd-2010-present-other-international-competition-fora/oecd-independent_sector_regulators_us.pdf

129 Federal Trade Commission, "About the FTC: What We Do," https://www.ftc.gov/about-ftc/what-we-do

130 Norm Alster, "Captured Agency: How the Federal Communications Commission Is Dominated by the Industries It Presumably Regulates," Edmond J. Safra Center for Ethics, June 23, 2015, https://ethics.harvard.edu/files/center-for-ethics/files/capturedagency_alster.pdf

131 Rick Claypool, "The FTC's Big Tech Revolving Door Problem," Public Citizen, May 23, 2019, https://citizen.org/article/ftc-big-tech-revolving-door-problem-report/

132 "H.R.4978 - Online Privacy Act of 2019," Congress.gov, December 18, 2019, https://www.congress.gov/bill/116th-congress/house-bill/4978/text

133 Harold Feld, "The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms," Roosevelt Institute and Public Knowledge, May 8, 2019, https://www.publicknowledge.org/assets/uploads/documents/Case_for_the_Digital_Platform_Act_Harold_Feld_2019.pdf

134 "The U.S. Urgently Needs a Data Protection Agency," Electronic Privacy Information Center, February 13, 2020, https://epic.org/dpa

135 "Statutes Enforced or Administered by the Commission," Federal Trade Commission, December 8, 2013, https://ftc.gov/enforcement/statutes.

136 Alex Propes, "Privacy & FTC Rulemaking Authority: A Historical Context," IAB, November 6, 2018, https://www.iab.com/news/privacy-ftc-rulemaking-authority-a-historical-context/

137 "FTC Announces Historic, Yet Insufficient, Settlement with Facebook for Privacy Violations," Open Technology Institution, July 24, 2019, https://newamerica.org/oti/press-releases/ftc-announces-historic-yet-insufficient-settlement-facebook-privacy-violations/

138 Nilay Patel, "Facebook's $5 billion FTC fine is an embarrassing joke," The Verge, July 12, 2019, https://theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke

139 "Privacy & Data Security: Update: 2019," Federal Trade Commission, March 6, 2020, https://ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf

140 42 U.S.C. § 2000ee

141 Garrett Hatch, "Privacy and Civil Liberties Oversight Board: New Independent Agency Status," Congressional Research Service, August 27, 2021 https://fas.org/sgp/crs/misc/RL34385.pdf

142 Becky Chao, Eric Null, and Claire Park, "Congress Could Design a New Data Protection Agency that Addresses Many of the Shortfalls of the FTC's Authority," Open Technology Institute, November 20, 2019, https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/congress-could-design-a-new-data-protection-agency-that-addresses-many-of-the-shortfalls-of-the-ftcs-authority

143 Data Accountability and Transparency Act of 2020," United States Senate Committee on Banking, Housing, and Urban Affairs, June 18, 2020, www.banking.senate.gov/imo/media/doc/Brown%20-%20DATA%202020%20Discussion%20Draft.pdf

144 Becky Chao, Eric Null, and Brandi Collins-Dexter, "Centering Civil Rights in the Privacy Debate," Open Technology Institute, Aug. 14, 2019, https://www.newamerica.org/oti/reports/centering-civil-rights-privacy-debate/

145 "The OECD Privacy Framework," Organization for Economic Co-operation and Development, August 17, 2014, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

146 Julie E. Cohen, "What Privacy is For," Harvard Law Review, June 22, 2015, https://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf

NEW AMERICA