The Discourse of Digital Privacy

An analysis of US and EU data protection policy

By

Martin Habrard

9,024 words

Submitted to

Central European University

Department of International Relations

In partial fulfilment of the requirements for the degree of

MA in International Relations (1 year)

Supervisor: Professor Xymena Kurowska

Vienna, Austria

2021

Abstract

The increase in data sharing/collection in recent decades has alerted policymakers to the need for data protection policy to preserve the right of individuals to digital privacy. However, not all data protection regimes have developed to the same degree and in the same way. This paper suggests that policy discourse surrounding the concept of digital privacy itself may be contributing to this disparity. To explore this question, it identifies the conceptual divide between the individualization and the collectivization of digital privacy and, by extension, data protection. It examines the discourse of forty US and EU policy texts along these lines. The analysis finds that EU discourse is considerably more collectivized, perhaps due to a more developed and consistent data protection regime and an emphasis on fundamental rights. On the other hand, US discourse is highly individualized, evidenced by consumer-oriented language and a focus almost exclusively on user control and consent policy. As well as impacting the success of new policy in their respective contexts, this discursive divide has implications for transatlantic cooperation on data protection. In short, the discrepancy between these two actors may seriously hinder cooperation on data protection, or at least restrict it to little more than the minimum acceptable level.

Acknowledgements

I would like to thank Xymena Kurowska for her invaluable support as supervisor of this project, as well as my beautiful Clémentine and our cat, Kiki, for making remote work a joy in this time of relative isolation.

Table of Contents

Introduction

With the rise of the data economy and increasingly invasive means of digital surveillance in the Western world, greater attention has been paid to the rights of individuals to digital privacy over the last few years. While liberal democratic states have shown the most interest in addressing this issue, there is no clear consensus as to where these rights begin and what the best means to protect them are. This is evidenced by the gulf in data protection between the United States and the European Union, for example. Despite several scandals such as the Snowden NSA leak and the more recent Cambridge Analytica scandal, data protection at the federal level in the US remains limited.[1] On the other hand, the EU has made considerably more progress with legislation such as the General Data Protection Regulation (GDPR).

The concept of digital privacy lies at the center of data protection policy. Some scholars have argued that it is either too narrowly or too loosely defined to appropriately deal with the complex issue of data protection.[2] Furthermore, assumptions about what digital privacy is or should be are inherently limiting from a policy standpoint, as they frame the way the question of data protection is approached. This does not necessarily lead to bad policy, but a better understanding of the conceptualization of privacy in this context is vital to critically evaluating the value of existing or proposed policies. It can also help explain the variation we see between different data protection regimes, such as in

[1] Group, Global Legal. "Data Protection 2020: Laws and Regulations: USA: ICLG." International Comparative Legal Guides International Business Reports. Global Legal Group. Accessed April 6, 2021. https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

[2] Bennett, Colin J. "In Defense of Privacy: The Concept and the Regime." S*urveillance & Society* 8, no. 4 (2011): 485–96. https://doi.org/10.24908/ss.v8i4.4184.

the US and the EU, and may provide some insight on the potential barriers to transatlantic cooperation on data protection. To this end, this study seeks to answer the following questions: How is the issue of digital privacy framed in policy discourse in the US and the EU? To what extent can different degrees of individualization and collectivization explain the discrepancy in data protection between the US and the EU? In response to these questions, a hypothesis is raised. If we posit that the discrepancy in data protection in the US and the EU is due to the greater political influence of private corporations in the US, then there may be evidence of this in US discourse in the form of a higher degree of individualization of privacy relative to the EU. Conversely, a more developed data protection regime in the EU suggests that policy discourse in that context is perhaps collectivized to a greater degree. In short, the dominance of individualized privacy discourse is expected to be detrimental, directly or indirectly, to data protection overall. Individualization and collectivization are discussed in greater detail throughout the literature review and in the section outlining the conceptual framework for this paper.

There are two main reasons why this research is important. The first is that it is necessary to understand the nature of a central concept like privacy, how it is defined and how this can affect policy. Of course, this is not an exercise for its own sake but is the first step in critically assessing the way that certain assumptions embedded in discourse limit the range of policy options. The second reason is that this discourse also impacts interstate relations on data protection. The non-physical nature of the internet means that digital privacy does not stop at state borders, and developed nations like the US and EU states, with high degrees of internet accessibility, have to work together to ensure both the protection of their citizens' rights and the smooth conduct of economic relations

despite different policy initiatives. Comparing US and EU discourse can provide some insight on what these two actors are likely to agree and disagree on when it comes to data protection.

Literature Review

Before going into the methodology, a review of the relevant literature is useful to contextualize its concepts and contributions. The literature on privacy is too broad and disjointed for this paper to be able to provide an appropriate review of the field in its entirety. Instead, this section focuses its attention to the literature on digital privacy discourse and policy over the last twenty to twenty-five years, with particular attention placed on relevant works from the last ten years or so. The more recent sources are obviously the more relevant in a rapidly changing technology and policy environment. These works generally constitute what Peppet calls the "new privacy scholarship," which is most notably characterized by its challenge to the "dominant" discourse of digital privacy and data protection. Naturally, these sources engage with and are themselves the products of decades of prior works on privacy. For example, the work of Alan Westin on privacy are briefly discussed, albeit through the lens of other works, since it represents one of the first and most significant descriptions of a paradigm that remains at the heart of data protection today. This section seeks to determine how the following questions are addressed in the aforementioned body of literature: How is (digital) privacy defined in public discourse? And why does this matter?

Data protection in the US and elsewhere cannot be fully understood without referring to what Alan Westin called the "privacy pragmatist" in his work on privacy in the 1960s and 70s.[3] "Privacy pragmatist" refers to the notion that the majority of people act as "rational consumers" when making decisions to disclose personal data in exchange

[3] Westin, Alan F. *Privacy and Freedom*. New York: Atheneum, 1970.

for goods and services.[4] Draper argues that the "rational consumer [is] at the center of debates about online privacy" today, which has created "a discursive lens that has informed debates about digital privacy in academic research […], policy negotiations […], and popular publications in the United States."[5] That this discourse has gained traction in the US and other liberal democracies is no surprise. As Draper notes, a notion of privacy centered on "individual reasoning and action […] is consistent with preferences for individual freedom and autonomy."[6] The most significant consequence of this discursive lens is that it has contributed to the "individualization" of digital privacy. The definition of privacy as "a function of individual choice" has been "operationalized through user control" in data protection policy aimed at protecting digital privacy.[7] This means that data protection policy has focused primarily on empowering individuals with the ability to decide whether or not to disclose their personal data to collectors. As Bietti's article suggests, the discourse of user control and consent is a vital part of EU data protection policy as seen through the recent GDPR, indicating that the individualistic notion of privacy embodied by the "privacy pragmatist" likely remains the dominant one in policy circles.[8]

According to Purtova, this discourse has also contributed to the "propertization" of personal data, especially in the US, which she describes as an attempt to counter the

[4] Draper, Nora A. "From Privacy Pragmatist to Privacy Resigned: Challenging Narratives of Rational Choice in Digital Privacy Debates." *Policy & Internet* 9, no. 2 (2016): 233. https://doi.org/10.1002/poi3.142.

[5] Ibid.

[6] Ibid., 243.

[7] Ibid., 236.

[8] Bietti, Elettra. *The Discourse of Control and Consent over Data in EU Data Protection Law and Beyond*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2001. https://www.hoover.org/research/discourse-control-and-consent-over-data-eu-data-protection-law-and-beyond

weak data protection regime in the US by incentivizing data collectors to respect privacy.[9] When data is defined as the personal property of individuals, they are potentially afforded greater control over its use. However, she claims that privacy is also a "social value" for which the market cannot account through property rights and user control regulations alone.[10] Byford agrees, arguing that propertization creates an "economic view of privacy" which is "overly reductionistic and disregards the underlying moral and social value of privacy."[11] Bietti also echoes this point. She says: "If privacy is a value strongly contingent on the interpersonal and social dimensions of collective life, then privacy self-management through choice and consent may be insufficient for regulating data and defining privacy's limits."[12] This is a common theme in the literature, and from here we can take a more detailed look at the authors' varied criticisms of the dominant paradigm described to this point.

First, several authors challenge the assumption that individuals is best placed to care for their own privacy. By shifting the conversation "away from structural change" in favor of user control, individuals are given a "new set of responsibilities" which they may not be able to manage appropriately.[13] This is because data protection then focuses primarily on an inherently unequal relationship. As Tzanou suggests, there are "inherent imbalances" in the relationship between "data subjects" and "data controllers."[14] For

[9] Purtova, Nadezhda. "Property Rights in Personal Data: Learning from the American Discourse." *Computer Law & Security Review* 25, no. 6 (2009): 508. https://doi.org/10.1016/j.clsr.2009.09.004.
[10] Ibid., 515.
[11] Byford, Katrin Schatz. "Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment." *Rutgers Computer and Technology Law Journal* 24, no. 1 (1998): 56.
[12] Bietti, *The Discourse of Control and Consent*, 5.
[13] Draper, "From Privacy Pragmatist to Privacy Resigned," 239 & 242.
[14] Tzanou, Maria. "Data Protection as a Fundamental Right next to Privacy? 'Reconstructing' a Not so New Right." *International Data Privacy Law* 3, no. 2 (2013): 91. https://doi.org/10.1093/idpl/ipt004.

example, individuals are often ignorant of industry practices like “interface design manipulation” that can allow them to collect more personal information than a “rational consumer” would consciously surrender.[15] At the heart of this issue is the fact that the rapid pace of technological change and the “opacity of the […] data ecosystem” make it difficult for most people to consistently make informed choices about their data.[16] Second, some authors claim that it is unrealistic to assume that the actions of individuals occur in isolation. For example, Bietti refers to the “privacy of the commons” concept when she claims that mass data processing means the consent of some individuals can impact the privacy of others.[17] In his work, Peppet argues that user control is naturally inadequate in a signaling economy that incentivizes the sharing of information.[18] The result is what he calls the “unraveling of privacy,” where social and economic pressure means people are likely to share information even when it would be detrimental to them.[19] In reference to Peppet’s argument, Draper notes that one individual’s choice can influence the choices of others despite not sharing the same “impulse nor the rewards of visibility.”[20] Third, the constant pressure on privacy and the complexity of the issue may simply discourage individuals from attempting to make informed decisions altogether. Draper’s main contribution is to introduce the concept of “resignation,” which she claims is the inevitable result of factors like unraveling and marketization which undermine privacy by incentivizing data disclosure.[21] As people become “resigned,” they passively opt into

[15] Bietti, *The Discourse of Control* and Consent, 1.
[16] Ibid., 5.
[17] Ibid.
[18] Peppet, Scott R. “Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future.” *Northwestern University Law Review*, 2011, 30.
[19] Ibid., 24.
[20] Draper, “From Privacy Pragmatist to Privacy Resigned,” 235.
[21] Ibid., 243.

programs or services at the expense of their digital privacy to avoid the potential "social or economic sanction" that could result from their abstention.[22] User-centric policies are also inherently discriminatory to underprivileged people without the time or knowledge to protect their personal data.[23] This is compounded by the tendency toward "social sorting" in data collection and data use which can have harmful political and economic effects on already vulnerable populations.[24] Finally, this discourse has the unfortunate and overarching effect of "making systemic privacy and data governance questions appear intractable," making the issue significantly harder to address despite the "persistent failure of the individual approach to privacy management."[25] Policy discourse is then more likely to entertain solutions that try to address the problem by simply reinforcing policies that are fundamentally inadequate.

While these criticisms represent valid concerns, they are of little value if they can't be used in the construction of a new paradigm in the service of better digital privacy management. Furthermore, it is impossible to conduct a policy analysis in search of collectivistic or "social good" privacy discourse without some concrete idea of the kind of policy it would entail. The following section looks at the more constructive aspects of the new privacy literature and serves to introduce some of the lines along which the aforementioned discourse analysis could be conducted. First, it should be noted that despite this trend in the privacy literature, most of the authors mentioned agree that user

[22] Ibid., 246.
[23] Ibid., 235.
[24] Bennett, "In Defense of Privacy," 490.
[25] Bietti, *The Discourse of Control and Consent*, 1. & Draper, "From Privacy Pragmatist to Privacy Resigned," 235.

control remains the prevalent paradigm in policy discourse. In other words, "[user] control dominates as the primary solution of privacy advocates."[26]

To start with broader prescriptions, Draper concludes her paper with a call to shift the paradigm away from personal responsibility and toward one which places the burden of protecting privacy more on the shoulders of "organizations."[27] Peppet tacitly supports this view by recognizing the value of a "theoretical shift" in addressing the weaknesses of the individual approach to privacy.[28] However, he also notes that user control is and will always be at the center of digital privacy since the individual remains the ultimate referent of the issue of privacy, pointing out that even the most critical authors still follow this logic.[29] Peppet even argues that the new privacy literature has reinforced the user control paradigm by neglecting to consider the harm done by "voluntary" disclosures of information.[30] Bennett suggests that the various conceptualizations of privacy he reviews in his work, which frame the issue in political and social terms, individually fail to do justice to the complexity of the concept.[31] To address this, he calls for some standardization of the concept and claims that this would, at the very least, help improve the strength of data protection policy in legislation and implementation.[32] He argues that this is especially important for policy discourse since the "most pressing challenge is with [the] enforcement and implementation" of data protection policy.[33] Bennett also notes that regardless of whether the individualistic notion of privacy is accurate, that the issue of digital privacy

[26] Peppet, "Unraveling Privacy," 31.
[27] Draper, "From Privacy Pragmatist to Privacy Resigned," 246.
[28] Peppet, "Unraveling Privacy," 36.
[29] Ibid.
[30] Ibid., 37.
[31] Bennett, "In Defense of Privacy," 490
[32] Ibid., 494.
[33] Ibid.

has been considered one of public policy suggests that it is, in fact, a social issue.[34] Byford argues that data protection should account for both the "personal and social value" of privacy."[35] She says: "Once deprivation of privacy is recognized as a matter of common societal concern, no individual member of the digital community can be free to deal away his privacy rights for mere financial or other gain."[36] This statement suggests that there should be some degree of privacy that is considered an inalienable right, though she does not clarify exactly where this line should be drawn. According to Byford, privacy is an important social issue because it plays a crucial role in the "facilitation of public participation and the formation of sociopolitical relationships."[37] Schwarz claims that information privacy is a "constitutive value" which shapes both society and "individual entities."[38] Byford sums up the concerns of the new privacy literature when she states that the protection of privacy as a social value is "as crucial to the creation of a viable information society as is the promotion of economic health."[39]

Her work is particularly interesting because it offers some relatively detailed policy suggestions. Since she tends to agree that data protection has largely been dominated by the individual approach, many of her prescriptions try to improve the way data protection policy protects the social value of privacy. According to Byford, the first step must be for "policymakers [to] expressly recognize the importance of privacy as a social concern […] and establish the institutional means of addressing the privacy problem."[40]

[34] Ibid., 490.
[35] Byford, "Privacy in Cyberspace," 57.
[36] Ibid.
[37] Ibid., 69.
[38] Schwartz, Paul M. "Internet Privacy and the State." *Connecticut Law Review* 32, no. 3 (2000): 834.
[39] Byford, "Privacy in Cyberspace," 69.
[40] Ibid.

Second, she says that data protection should not only include "notice and consent requirements" but should also require data collectors to explicitly justify their activities.[41] Furthermore, she argues that data collectors should bear the responsibility of examining "the purposes and effects of their data gathering activities" and should be made to "refrain from soliciting information" without a "justifiable purpose for data collection."[42] On the former point, it seems unlikely that data collectors would produce the most reliable studies on the effects of their activities, but this could at least help to reduce the opacity of the data collection process by having data collectors researching and publishing the effects of their activities as an industry standard. On the question of justification, Schwarz makes a related argument. He states: "information privacy norms should create shifting, multidimensional data preserves that insulate personal data from different kinds of observation by different parties."[43] The call for this layered notion of privacy assumes that some actors are justified in collecting certain kinds of data even when other are not, in which case a blanket privacy protection regime would be unnecessary. However, this does not preclude the need for explicit justification and transparency in the process, so Byford and Schwarz's points are certainly compatible. Byford's last point is that consumers should be "fully inform[ed]" of the "underlying reasons for information requests and of their concomitant privacy rights."[44] This is probably the aspect of data protection that has gotten the most attention in EU and US policy circles in the time since Byford's work, which is no surprise considering that, unlike her other prescriptions, it fits squarely with the individual approach to privacy protection.

[41] Ibid., 71.
[42] Ibid.
[43] Schwartz, "Internet Privacy and the State," 834.
[44] Byford, "Privacy in Cyberspace," 72.

The fact that individualization and collectivization are not strictly opposed in policy terms is a possible source of confusion. However, they are conceptually dichotomous and can lead to drastically divergent policy. Most of the authors discussed in this section argue that the focus on user control is ineffective or harmful. Despite their work, these concepts remain poorly defined. Furthermore, while some scholars like Bietti have examined more recent cases like the GDPR for individualistic discourse, little work has been done to see if collectivized privacy discourse has had any impact on policy in recent years. Again, this is likely due, at least in part, to the lack of definition of these concepts in concrete terms. In the following section, this paper attempts to define them in order to form the base from which said analysis is performed. The contributions of this paper to the privacy literature are twofold. First, it seeks to develop the conceptualization of data protection policy as it relates to privacy as a social value. Second, it aims to determine the extent to which the collectivization of privacy in the literature has been reflected in policy developments in the US and EU in recent years, or if privacy remains starkly individualized in either contest. Through this research it hopes to draw some conclusions about the prevailing socio-economic factors acting upon privacy management in either context, as well as draw some insight on what this means for transatlantic relations on data protection.

Methodology

Conceptual Framework

As a brief note, the concerns of some authors like Fuster and Tzanou concerning the conflation of data protection with digital privacy should be addressed. In short, they argue that these terms are widely and incorrectly considered to be two sides of the same thing, ignoring the broader definitions of both privacy and data protection.[45] This can also have implications on the discourse of data protection, but is not the subject of this paper. While distinguishing between data protection and digital privacy is potentially important, this paper simply adopts the instrumentalist approach described by Tzanou, which assumes that data protection refers to the legislative measures with which digital privacy can be protected.[46] This is not likely to pose a significant problem since this analysis focuses generally on cases which are explicitly concerned with digital privacy.

Moving on, this study is not the first to discuss the way digital privacy is defined in policy discourse and benefits from the existence of a number of studies which discuss the discursive divide between the individualization and the collectivization of digital privacy, along which the analysis is conducted. The individualization side of this debate is undeniably the most developed of these two concepts. To reiterate, "individualization" refers to the assumption that digital privacy refers to the privacy of individuals and, consequently, that data protection should focus on empowering individuals with the

[45] González Fuster, Gloria. "The Emergence of Personal Data Protection as a Fundamental Right of the EU." *Law Governance and Technology Series* 16 (2014): 1-272. & Tzanou, "Data Protection as a Fundamental Right."

[46] Tzanou, "Data Protection as a Fundamental Right," 91.

knowledge and tools to protect their data. Discourse which individualizes digital privacy encourages policy that strengthens user control and disclosure of data collection and use. By shifting responsibility from data collectors to individual users, the individualization of digital privacy acts as an extension of the general trend toward individualism in capitalist-oriented societies.[47] This is why it is assumed that discourse which individualizes the issue is expected to be more salient in the American context, but other studies suggest that the EU data protection regime, though more developed, also leans heavily on individual-centric policies.[48]

Individualization can be contrasted with more collectivistic conceptions of digital privacy which, for example, prioritize "encoding data protection by design and by default in platform infrastructures" which "reduce the burden on individual users and lead to fairer data governance."[49] This view implies that individuals are ultimately limited in the power they have to protect their own privacy. Furthermore, there is a difference in how digital privacy is defined as a right. Preliminary research suggests that digital privacy is often either defined as a consumer right or a fundamental human right. While it can be argued that consumer rights are, in fact, a subset of human rights, framing the issue of digital privacy as one that primarily concerns consumers makes data protection appear less like a human rights issue and more like an issue of business ethics. This may not seem significant, but the fact is that consumer rights have not been universally accepted as

[47] Kennedy P. "Individualization and the Cultures of Capitalism." In: *Vampire Capitalism*. Palgrave Macmillan, London, 2017. https://doi.org/10.1057/978-1-137-55266-2_6

[48] Bietti, "The Discourse of Control and Consent."
[49] Ibid., 2.

human rights.[50] Therefore, discourse which makes consumers the primary subjects of data protection is not likely to demand the same standards of regulation as it would to prevent a human rights violation.

As seen in Table I, a metric has been created based on these concepts and the discussion on digital privacy discourse in the literature. While the different elements on either side of the metric are based on the discursive divide discussed in earlier sections, they are not mutually exclusive in policy terms. Therefore, determining where a given case of policy text lies on this scale inevitably relies on a subjective case-by-case analysis that weighs the relative salience of these elements against one another.

Table I.

Individualization	**Collectivization**
Individuals are the primary *subjects* of data protection. They are rational consumers and digital privacy is a *consumer right*. Personal data is the extension of personal property.	While individuals may still be at the center of policy, their right to digital privacy is a fundamental *human right*. Furthermore, digital privacy is an *interpersonal and social value* which needs to be protected.
Digital privacy is ultimately the *responsibility* of data subjects, so individuals are responsible for their personal data. They are free to disclose all of their personal data to any actor as long as the decision is *voluntary* and sufficiently *informed*.	Data collectors and the state bear the *responsibility* of limiting the unnecessary collection of personal data. There are *limitations* on the freedom of individuals to disclose personal data.

[50] Brenkert, George G. "Business Ethics and Human Rights: An Overview." *Business and Human Rights Journal* 1, no. 2 (2016): 277–306. https://doi.org/10.1017/bhj.2016.1.

Data protection policy is primarily concerned with improving *user control* over the way their personal data is used by allowing them to give or withhold informed *consent* to data collectors.	Data protection policy emphasizes the responsibility of data collectors to *justify* data collection and to *refrain* from collecting data without justification. Data collectors are responsible for *monitoring* and *limiting* the harmful effects of data collection.

Research Design

A simple grading system is used to help categorize, quantify, and visualize the findings of the analysis based on the scale represented in Table I. It is not symmetrical in the sense that individualization is assumed to be dominant to begin with and is impossible to exclude when discussing digital privacy. The grading scale is as follows: a score of 2 represents the highest degree of collectivization, with strong elements of collectivization in both the discourse itself and the policy recommendations. A score of 1 is assigned to a text in which there are a number of notable collectivized elements but where individualization still dominates overall. Finally, a score of 0 describes a text with no collectivization. Scores are also given up to one decimal point to allow for a more precise interpretation of where the texts lie on the scale. Ideally, a score of zero would represent an example of policy discourse which argues that individuals should be entirely responsible for their digital privacy, such as by abstaining from using certain services or devices. However, even in a highly individualized policy discourse environment like the US, the standard is that some degree of government regulation is required to protect the rights of individuals. Therefore, a score of zero here represents the baseline that is existing privacy regulation. Alongside having no other collectivized elements, a policy text would need to recommend no increase in federal protection at all to earn a score of zero.

Since the general trend is for increased protection, however minimal or individualized, a score of zero is highly unlikely in this context. The main limitation of this part of the analysis is that the grading process is vulnerable to selection (confirmation) bias. The discussion on the findings are supported with examples from the texts in an effort to provide an accurate representation of their content, but this should still be taken into consideration.

Once policy texts are analyzed individually and their scores compiled, the EU and US samples are compared to see whether the difference in discourse aligns with the transatlantic discrepancy in data protection. The discussion section presents the findings from the US sample and the EU sample consecutively, with comparisons made throughout. This is followed by a brief discussion of the implications of these findings for transatlantic cooperation on data protection. If policy discourse is found to be either equally individualistic or collectivistic in both the US and the EU, then an argument based on these factors would not explain the difference in policy between them. While the same variables may still be the root cause of the issue, there may be other ways in which they are affecting the end result that is data protection policy. If the EU discourse is found to be more individualistic than the US, then this would undermine the hypothesis that the individualization of digital privacy is detrimental to data protection. Conversely, the reverse would satisfy the hypothesis and would suggest that these elements, whatever their origins, may be restricting and propelling data protection policy in the US and the EU, respectively.

Case Selection

To start, this analysis focuses exclusively on policy texts released over the last ten years or so, with the majority having been released in the latter half of the last decade. These texts represent the most recent developments in data protection policy in the US and the EU, allowing this analysis to build upon the work of other authors in the digital privacy literature with a minimal amount of overlap. Moving on to sample size, this paper analyzes two sets of twenty sources for a total of forty policy texts, divided evenly between the US and the EU.

The EU context includes a number of easily identifiable cases which could provide source material for a discourse analysis. The most obvious is the *General Data Protection Regulation* (GDPR).[51] There are also a number of cases related to the European Data Protection Supervisor (EDPS), the primary supervising authority for data protection in the EU. This includes the negotiations with non-EU states on Passenger Name Record (PNR) data, the opinion published by the EDPS in April of 2016 relating EU-Canada PNR negotiations being an example.[52] More recently, the EDPS has also published a joint opinion on the proposed Data Governance Act.[53] Other examples include EDPS strategy papers and a variety of EDPB opinion papers released over the last few years.

[51] "Official Legal Text." General Data Protection Regulation (GDPR), September 2, 2019. https://gdpr-info.eu/.

[52] "EDPS Pleading at the Hearing of the Court of Justice, EU-Canada PNR Agreement." European Data Protection Supervisor. Accessed April 5, 2021. https://edps.europa.eu/data-protection/our-work/publications/court-cases/edps-pleading-hearing-court-justice-eu-canada-pnr_en.

[53] European Data Protection Supervisor (EDPS). *EDPB-EDPS Joint Opinion on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*. 2021. https://edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-opinion-proposal-regulation-european_en.

Data protection in the US offers fewer cases for analysis, especially at the federal level, but a look at federal data protection in the US would not be complete without examining the role of the Federal Trade Commission (FTC). Although it does not deal exclusively with data protection, the FTC is the primary federal body with authority on the subject due to its role in protecting American consumers by regulating against "deceptive practices" in commercial practice. [54] For example, the Do Not Track Act of 2011 provides an interesting case, on which the FTC has published a number of documents such as the *Prepared Statement of the Federal Trade Commission on The State of Online Consumer Privacy Before the Committee on Commerce, Science, and Transportation* given to the US Congress in March of 2011.[55] The Do Not Track Act provides a number of policy documents, including several from the FTC, which offer excellent material from which to conduct the analysis. As one of the few pieces of data protection legislation at the federal level, this case is likely to provide a good overview of policy discourse in the US on the subject. To supplement the lack of existing policy on the subject, the US sample is also bolstered by a number of proposed pieces of legislation which were introduced to Congress over the last few years, as well as various statements from two Congressional hearings on data protection.

[54] Group, Global Legal. "Data Protection 2020."

[55] U.S. Federal Trade Commission. *Prepared Statement of the Federal Trade Commission On The State of Online Consumer Privacy*. Washington D.C.: 2019. https://www.ftc.gov/public-statements/2011/03/prepared-statement-federal-trade-commission-state-online-consumer-privacy

Results and Discussion

Table IIa.

US Source	Grade
1. FTC: Do Not Track[56]	0.5
2. FTC: Painting the Privacy Landscape[57]	0.2
3. Congressional Hearing: "Oversight of the Federal Trade Commission," FTC Prepared Statement[58]	0.2
4. Congressional Hearing: "Oversight of the Federal Trade Commission," Opening Statement by Chairman Frank Pallone, Jr.[59]	0.3
5. Congressional Hearing: "Oversight of the Federal Trade Commission," Opening Statement by Chair Jan Schakowsky[60]	0.2
6. Senate Committee of Commerce, Science, and Transportation: The State of Online Privacy and Data Security by Ranking Member Maria Cantwell[61]	0.2

[56] U.S. Federal Trade Commission. *Prepared Statement of the Federal Trade Commission on Do Not Track Before the Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, United States House of Representatives*. Washington D.C.: 2010. https://www.ftc.gov/public-statements/2010/12/prepared-statement-federal-trade-commission-do-not-track

[57] U.S. Federal Trade Commission. *Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases*. Maureen K. Ohlhausen. Washington D.C.: 2010. https://www.ftc.gov/public-statements/2017/09/painting-privacy-landscape-informational-injury-ftc-privacy-data-security

[58] U.S. Federal Trade Commission. *Prepared Statement of the Federal Trade Commission: Oversight of the Federal Trade Commission Before the Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce, United States House of Representatives*. Washington D.C.: 2019. https://energycommerce.house.gov/committee-activity/hearings/hearing-on-oversight-of-the-federal-trade-commission-strengthening

[59] U.S. Congressional Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce. *Opening Statement*. Chairman Frank Pallone, Jr. Hearing on "Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security." Washington D.C.: 2019. https://energycommerce.house.gov/newsroom/press-releases/pallone-remarks-at-ftc-oversight-hearing-0

[60] U.S. Congressional Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce. *Opening Statement*. Chair Jan Schakowsky. Hearing on "Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security." Washington D.C.: 2019. https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/2019.5.8.SCHAKOWSKY.%20FTC%20Oversight%20Hearing.CPC__0.pdf

[61] U.S. Senate Committee of Commerce, Science, and Transportation. *The State of Online Privacy and Data Security*. Ranking Member Maria Cantwell. Washington D.C.: 2010. https://www.cantwell.senate.gov/imo/media/doc/The%20State%20of%20Online%20Privacy%20and%20Data%20Security.pdf

7. Online Privacy Act of 2019[62]	1.0
8. Consumer Online Privacy Rights Act[63]	0.3
9. Data Protection Act of 2020[64]	0.6
10. Congressional Hearing: "Examining Legislative Proposals to Protect Consumer Data Privacy," Majority Statement by Chairman Roger Wicker[65]	0.1
11. Congressional Hearing: "Examining Legislative Proposals to Protect Consumer Data Privacy," Minority Statement by Ranking Member Maria Cantwell[66]	0.2
12. Congressional Hearing: "Examining Legislative Proposals to Protect Consumer Data Privacy," Written Testimony of Julie Brill[67]	1.2
13. Congressional Hearing: "Examining Legislative Proposals to Protect Consumer Data Privacy," Written Testimony of Maureen Ohlhausen[68]	0.2
14. Congressional Hearing: "Examining Legislative Proposals to Protect Consumer Data Privacy," Written Testimony of Laura Moy[69]	1.3
15. Congressional Hearing: "Examining Legislative Proposals to Protect Consumer Data Privacy," Written Testimony of Nuala O'Connor[70]	0.1

[62] H.R.4978 - Online Privacy Act of 2019. Bill introduced to the 116th U.S. Congress (2019).

[63] S.2968 - Consumer Online Privacy Rights Act. Bill introduced to the 116th U.S. Congress (2019).

[64] S.3300 - Data Protection Act of 2020. Bill introduced to the 116th U.S. Congress (2020).

[65] U.S. Senate Committee on Commerce, Science, and Transportation. *Majority Statement*. Chairman Roger Wicker. Hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy." Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

[66] U.S. Senate Committee on Commerce, Science, and Transportation. *Minority Statement*. Ranking Member Maria Cantwell. Hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy." Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

[67] U.S. Senate Committee on Commerce, Science, and Transportation. *Written Testimony*. Julie Brill. Hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy." Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

[68] U.S. Senate Committee on Commerce, Science, and Transportation. *Written Testimony*. Maureen Ohlhausen. Hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy." Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

[69] U.S. Senate Committee on Commerce, Science, and Transportation. *Written Testimony*. Laura Moy. Hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy." Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

[70] U.S. Senate Committee on Commerce, Science, and Transportation. *Written Testimony*. Nuala O'Connor. Hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy." Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

16. Congressional Hearing: "Examining Legislative Proposals to Protect Consumer Data Privacy," Written Testimony of Michelle Richardson[71]	1.4
17. Discussion Draft The United States Consumer Data Privacy Act (USCDPA)[72]	0.3
18. The Privacy Bill of Rights Act of 2019[73]	0.5
19. Public Interest Privacy Legislation Principles[74]	0.9
20. Center for Democracy and Technology (CDT)'s Federal Baseline Privacy Legislation Discussion Draft[75]	0.6
	Average: 0.515

Table IIa shows the grades assigned to twenty US policy texts on data protection over the last ten years. These include a number of different cases, but they are all concerned with the question of general federal data protection in the United States. The vast majority of these texts come from 2019 or later, which can be traced in part to growing public concern over digital privacy in the wake of the 2018 Cambridge Analytica scandal.[76] The sources include two FTC statements, a number of statements from two Congressional hearings, four pieces of legislation introduced to Congress and one draft legislation, two sources taken directly from public interest groups, and an additional

[71] U.S. Senate Committee on Commerce, Science, and Transportation. *Written Testimony*. Michelle Richardson. Hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy." Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

[72] U.S. Senate Committee on Commerce, Science, and Transportation. *Discussion Draft of the United States Consumer Data Privacy Act*. Chairman Roger Wicker. Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/chairman-wicker-s-discussion-draft-the-united-states-consumer-data-privacy-act

[73] S.1214 - Privacy Bill of Rights Act. Bill introduced to the 116th U.S. Congress (2019).

[74] "Principles for Privacy Legislation." New America, November 13, 2018. https://www.newamerica.org/oti/press-releases/principles-privacy-legislation/.

[75] "CDT's Federal Baseline Privacy Legislation Discussion Draft." Center for Democracy and Technology, July 20, 2020. https://cdt.org/insights/cdts-federal-baseline-privacy-legislation-discussion-draft/.

[76] H.R.4978 - Online Privacy Act of 2019, 2019.

statement by the ranking member of the Senate Committee Science, Commerce, and Transportation.

The results shown on Table IIa suggest that US policy discourse is strongly individualized. This is consistent with the hypothesis raised at the start of the paper. Many texts contained a minimal amount of collectivization and only a handful reached the degrees seen in most EU sources, which becomes clearer as we discuss EU discourse later on. The clearest indication of an economic focus is the dominance of consumer-related discourse in these texts. Roughly 17 out of 20 refer to data subjects primarily as "consumers" with the object of data protection being to protect consumer rights. Of the three exceptions, two are the sources from public interest groups, numbered 19 and 20 in Table IIa, and the third is the Privacy Bill of Rights Act of 2019. This lowered the scores of the texts numbered 1 through 17 considerably, but it did not preclude them from scoring relatively highly. Some of the highest scores, such as the one assigned to the testimony of Microsoft's Julie Brill, were given despite the dominance of consumer related discourse.

The Federal Trade Commission (FTC) is a vital part of the discussion because, as mentioned earlier, it is the main federal government body responsible for data protection in the United States. Consequently, the body of sources selected for the analysis includes two texts published by the FTC as well as three texts related to a Congressional hearing titled "Oversight of the Federal Trade Commission" by the Senate Committee on Commerce, Science, and Transportation which took place on May 8, 2019. The central role of the FTC in US data protection is both evidence of and a contributing factor to the pervasiveness of this economic view of digital privacy in US policy discourse.

Furthermore, the US Senate Committees and subcommittees tasked with dealing with privacy issues are also those that otherwise deal with issues of "commerce" or the economy.

Framing the issue as one that is economic in nature goes deeper than simply referring to data subjects as consumers. The discourse also focuses almost exclusively on the relationship between consumers and data collectors, the latter designation generally referring to private corporations. Policymakers often express the need to avoid stifling the data economy through overly harsh and complicated regulations. Data sharing is described as a benefit to both individuals and corporations, and the main purpose of data protection is taken to be to ensure consumer trust without hindering economic performance. According to former Chairman Roger Wicker of the Senate Committee on Commerce, Science, and Transportation, data protection should consist of "a strong, national, and preemptive privacy law that provides consumers with certainty," while taking care not to negatively impact "product development and innovation, or what content a consumer is able to view or engage with online."[77] In order to satisfy this balance between the protection of consumer rights and economic performance, proposed policy solutions almost always revolve around empowering individuals with greater control over their personal data. As an example, let us look at the measures proposed in the Consumer *Online Privacy Act of 2019*. It seeks to grant a number of rights to individuals regarding their personal data, including the following: "[t]he right to access their data and greater transparency […]. The right to control the movement of their data which gives consumers

[77] *Majority Statement*. Chairman Roger Wicker. Hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy," 2019.

the ability to prevent data from being distributed to unknown third parties. The right to delete or correct their data. The right to take their data to a competing product or service."[78] While US discourse often stresses that data collectors should take greater responsibility in protecting digital privacy, this generally refers to the responsibility to provide users with the tools and information needed to make informed decisions. The concern of US policymakers and other actors with discrimination in the data economy is probably the closest thing which mirrors EU rights-based discourse. For example, the *Consumer Online Privacy Rights Act* was drafted in part to "safeguard civil rights by creating new enforcement powers for the Federal Trade Commission to take action against unlawful discrimination in the digital economy."[79] This is a common thread in many texts, but it rarely exceeded being a note as part of the decentralized, user-centered approach. As a result, the call for corporate responsibility and anti-discrimination policies hardly constitute a break from the individualized approach. Since US policy discourse revolves around the relationship between individuals and consumers, it rarely discusses the wider social implications of data-sharing. There is no reference to a codified and general right to privacy, so the justification for increased data protection stems from growing consumer demand following specific cases of privacy breaches like the Cambridge Analytica scandal. This might explain the surge in proposed data protection regulations in 2019 and why none of these were ultimately successful.

It is also worth examining how the role of the state in privacy management is represented in the sample. FTC sources tend to have the weakest notion of state

[78] S.2968 - Consumer Online Privacy Rights Act, 2019.

[79] S.2968 - Consumer Online Privacy Rights Act, 2019.

responsibility. While FTC officials recognize the need for stronger privacy protection and greater standardization of policy at the federal level, the data protection regime they envision is a decentralized one where the state ideally abstains from taking an active role. In this "self-regulatory" framework, the role of state policy is to "guide and motivate industry as it develops more robust and effective best practices and self-regulatory guidelines."[80] Proposed legislations like the *Online Privacy Act of 2019* tend to envision greater state responsibility than the "self-regulatory" approach of the FTC, such as through proposing the creation of a data protection agency to fulfill this role. Other pieces of proposed legislation, such as the *Data Protection Act of 2020*, are also slightly more collectivized in that they placed a greater emphasis on measures promoting data minimization.[81] However, it should also be noted that these bills, numbered 7 through 9 and 18 in Table IIa, were introduced to Congress but failed to even get a vote and were discarded at the end of the 116th Congress in January 2021. Therefore, while they certainly serve as examples of US policy discourse on data privacy, they do not reflect the actual state of US federal data protection.

Also included in the analysis are a number of texts that do not come from policymakers directly. For example, the Congressional hearings involved the testimony from a diverse array of actors ranging from corporate executives, academics, and the representatives of public interest groups. While these texts stretch the definition of "policy discourse," they come from actors that were called as witnesses to Congressional hearings. These individuals represent some of the most relevant non-government actors

[80] FTC. *Prepared Statement of the Federal Trade Commission on Do Not Track*, 2010.
[81] S.3300 - Data Protection Act of 2020, 2020.

in US data protection, and, since policymakers intend to use this information to make informed decisions on how to proceed with data protection legislation, their discourse is likely to have a direct impact on policy implementation. Analyzing these sources also has the potential to reveal aspects of policy discourse that deviate from or are otherwise absent from that of policymakers, so it comes as no surprise they contain some of the highest levels of collectivization in the US sample. Notably, it is among these sources that we find the only mentions of digital privacy as a fundamental human right. Michelle Richardson, the Director of the Privacy & Data Center for Democracy & Technology, stated: "CDT is committed to protecting privacy as a fundamental human and civil right and as a necessity for securing other rights such as access to justice, equal protection, and freedom of expression."[82] Ironically, this position is also mirrored by a representative of a private corporation. Microsoft executive and Former FTC Commissioner Julie Brill claimed that Microsoft "believe[s] that privacy is a fundamental human right and that, with recent advances in technology, the protection of this right has become more important and more urgent than ever before."[83] Additionally, the presence of other strongly collectivized discourse in Julie Brill's statement, including the call for greater corporate responsibility, data collection justification, and stronger federal legislation, made it one of the highest scoring texts in the sample. The written testimony of Executive Director of the Georgetown Law Center on Privacy, Laura Moy, is also interesting in that, despite consumer-oriented language, it closely mirrors many of the critical arguments of the privacy literature. For example, Moy makes perhaps the strongest critique of the user-

[82] *Written Testimony*. Michelle Richardson. Hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy," 2019, 1.

[83] *Written Testimony*. Julie Brill. Hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy," 2019, 5.

centered approach in the sample when she argues that "[t]he consent model also has reached the limits of scalability and is no longer feasible as a practical matter."[84] Furthermore, she makes a rare comment on the social benefit of data protection, claiming that "data-driven distribution models […] can lead to a number of harms not only to individual consumers, but to society more broadly."[85] This is to be expected from an academic source, but its relative uniqueness in the Congressional hearing and in the sample more broadly make it interesting, nonetheless. This marks the conclusion of the section on US discourse; the following section takes a turn to the EU sample.

Table IIb.

EU Source	Grade
1. EDPS Strategy 2013-2014[86]	1.2
2. EDPS Strategy 2015-2019[87]	0.5
3. EDPS 2015-2019: Leading by Example - Executive Summary[88]	1.7
4. EDPS Annual Management Plan 2019 – Summary[89]	1.5

[84] *Written Testimony*. Laura Moy. Hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy," 2019, 2.

[85] Ibid., 4-5.

[86] European Data Protection Supervisor (EDPS). *Strategy 2013-2014: Towards excellence in data protection*. Luxembourg: Publications Office of the European Union: 2012. https://edps.europa.eu/data-protection/our-work/publications/strategy/strategy-2013-2014_en

[87] European Data Protection Supervisor (EDPS). *The EDPS Strategy 2015-2019: Leading by Example*. Luxembourg: Publications Office of the European Union: 2015. https://edps.europa.eu/data-protection/our-work/publications/strategy/strategy-2015-2019_en

[88] European Data Protection Supervisor (EDPS). *Leading by Example - EDPS 2015-2019 - Executive Summary*. Luxembourg: Publications Office of the European Union: 2019. https://op.europa.eu/webpub/edps/edps-2015-2019-executive-summary/en/

[89] European Data Protection Supervisor (EDPS). *Promoting a new culture of data protection: Annual Management plan 2019 – Summary*. Luxembourg: Publications Office of the European Union: 2019. https://edps.europa.eu/press-publications/publications/strategy_en

5. EDPS Strategy 2020-2024[90]	2.0
6. EDPB Opinion on the adequate protection of personal data in Japan[91]	1.0
7. EDPB Recommendations on the adequacy referential under the Law Enforcement Directive[92]	1.6
8. EDPS Annual Report 2016 – Executive Summary[93]	1.3
9. EDPS Annual Report 2017 – Executive Summary[94]	1.3
10. EDPS Annual Report 2018 – Executive Summary[95]	1.9
11. EDPS Annual Report 2020 – Executive Summary[96]	1.4
12. EDPS Opinion 1/15 on the draft EU-Canada PNR agreement[97]	1.1
13. EU Council proposal for a directive on the use of passenger name record data for law enforcement purposes[98]	1.1
14. EDPB-EDPS Joint Opinion on the Proposal for a regulation of the European Parliament and of the	1.5

[90] European Data Protection Supervisor (EDPS). *The EDPS Strategy 2020-2024: Shaping a Safer Digital Future*. 2020. https://edps.europa.eu/data-protection/our-work/publications/strategy/edps-strategy-2020-2024-shaping-safer-digital-future_en

[91] European Data Protection Board (EDPB). *Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan*. https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-282018-regarding-european-commission-draft_en

[92] European Data Protection Board (EDPB). *Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive*, 2021. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_en

[93] European Data Protection Supervisor (EDPS). *Annual Report 2016 - Executive Summary.* Luxembourg: Publications Office of the European Union, 2017. https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2016-annual-report-state-privacy-2017-edps_en

[94] European Data Protection Supervisor (EDPS). *Annual Report 2017 - Executive Summary.* Luxembourg: Publications Office of the European Union, 2018. https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2017-annual-report-data-protection-and-privacy_en

[95] European Data Protection Supervisor (EDPS). *Annual Report 2018 - Executive Summary.* Luxembourg: Publications Office of the European Union, 2019. https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2018-annual-report-new-era-data-protection_en

[96] European Data Protection Supervisor (EDPS). *Annual Report 2020 - Executive Summary.* 2021. https://edps.europa.eu/data-protection/our-work/publications/annual-reports/annual-report-2020_en

[97] European Data Protection Supervisor (EDPS). *EDPS Pleading at the Hearing of the Court of Justice, EU-Canada PNR Agreement*. 2016. https://edps.europa.eu/data-protection/our-work/publications/court-cases/edps-pleading-hearing-court-justice-eu-canada-pnr_en.

[98] Council of the European Union. *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*. 2011. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52011PC0032

Council on European data governance (Data Governance Act)[99]	
15. EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)[100]	1.9
16. European Commission Proposal for the Regulation on Privacy and Electronic Communications (ePrivacy Directive)[101]	1.2
17. European Commission Staff Working Document - Executive Summary of the Ex-post REFIT evaluation of the ePrivacy Directive[102]	1.4
18. European Commission to the EU Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation[103]	1.3
19. European Commission to the EU Parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond – taking stock[104]	1.2
20. General Data Protection Regulation (GDPR)[105]	1.3
	Average: 1.37

[99] European Data Protection Supervisor (EDPS*). EDPB-EDPS Joint Opinion on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*. 2021.

[100] European Data Protection Supervisor (EDPS). *EDPS Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*. 2017. https://edps.europa.eu/data-protection/our-work/publications/opinions/eprivacy-regulation_en

[101] European Commission. *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*. Brussels: 2017. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications

[102] European Commission. *Commission Staff Working Document - Executive Summary of the Ex-post REFIT evaluation of the ePrivacy Directive*. Brussels: 2017. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications

[103] European Commission. *Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*. Brussels: 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264

[104] European Commission. *Communication from the Commission to the European Parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond – taking stock*. Brussels: 2019. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2019:0374:FIN

[105] "Official Legal Text." General Data Protection Regulation (GDPR), September 2, 2019. https://gdpr-info.eu/.

With a greater number of advisory or legislative bodies concerned with data protection at the EU level, EU policy texts on the subject tend to be easier to find. As a result, the EU sample does not rely on sources from actors other than policymakers. This may contribute to the convergence of EU policy discourse across the various texts. However, the composition of the EU sample is the result of a more developed and consistent body of policy on data protection at the EU level, so it remains a representative sample.

The degree to which US discourse individualizes digital privacy only becomes clear when we contrast it to its EU counterpart. As shown in Table IIb, the average grade assigned to EU scores was 1.37, considerably higher than the US average at 0.515. The clearest contributor to the raising of the baseline of EU scores is the consistency of and insistence on the protection of digital privacy as a fundamental right of EU citizens. In contrast to the US where rights-based discourse is limited to anti-discrimination policy, the fundamental right to privacy often acts as the starting point for EU texts when discussing the need for data protection. Furthermore, the consistency of this language stems from the codification of the fundamental right to privacy in the EU Charter, something unseen in US policy discourse on the subject. For example, a 2017 executive summary of the EU Commission Staff Working Document evaluating the ePrivacy Directive states the following: “It aims to ensure that the protection of confidentiality of communications, in line with the fundamental right to the respect of private and family life enshrined in Article 7 of the EU Charter of Fundamental Rights, is guaranteed.”[106] While

[106] European Commission. *Commission Staff Working Document - Executive Summary of the Ex-post REFIT evaluation of the ePrivacy Directive*, 2.

it is not always mentioned directly, the consistent use of the term “fundamental rights” is in clear reference to the EU Charter.

Even though this discursive trend is the most visible difference between the EU and the US, it does not necessarily mean that data protection policy is any less individualized. However, by broadening the notion of digital privacy, it does seem to contribute to a more a collectivized data protection regime in the EU. While consumer-related discourse focuses on the relationship between individuals and private corporations, the concern with fundamental rights extends beyond the commercial aspect of digital privacy. Data protection in the EU seeks to protect the fundamental rights of individuals from actors other than private corporations and in contexts other than economic activity, such as data collection for law enforcement purposes. For example, the EDPB recommends that for data processing by law enforcement authorities to respect these fundamental rights, it should be justified as “necessary […] for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.”[107] Similarly, the EDPS states in its 2017 Opinion on the “ePrivacy Regulation” that the “central legal function” of Article 7 of the EU Charter is “the protection of the fundamental right to privacy against any interference, especially from state authorities.”[108]

Another common thread in EU policy discourse is that EU policymakers stress the broader social and political importance of data protection. In both sources numbered 4

[107] European Data Protection Board (EDPB). *Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive*, 10.

[108] European Data Protection Supervisor (EDPS). *EDPS Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*.

and 5 in the EU sample, the EDPS claims that data protection is essential to preserving the health of democratic society in the digital age.[109] In a review of data protection under the GDPR two years after its implementation, the EU Commission specifically mentions the threat of data processing and disinformation to democracy. It states: "Protecting personal data is also instrumental in preventing the manipulation of citizens' choices, in particular via the micro-targeting of voters based on the unlawful processing of personal data, avoiding interference in democratic processes and preserving the open debate, the fairness and the transparency that are essential in a democracy."[110] In the executive summary of its *Leading by Example* paper covering the period from 2015-2019, the EDPS argues that: "The Facebook/Cambridge Analytica scandal in 2018 revealed the fragility of our democracy, where the public sphere has shifted onto a complex, unaccountable matrix of tracking, profiling and targeting."[111] This is in sharp contrast to some examples in US discourse, such as the *Online Privacy Act of 2019*, which describe the scandal primarily as a violation of consumer confidence.[112]

In a concrete policy sense, the best example of collectivized discourse in EU texts is the consistent inclusion of the notion of "privacy-by-design," which is significant because it implicitly challenges the assumption that user control and consent measures are sufficient for an adequate level of data protection. For example, the EDPS

[109] European Data Protection Supervisor (EDPS). *Annual Management plan 2019 – Summary*, 2. & European Data Protection Supervisor (EDPS). *The EDPS Strategy 2020-2024: Shaping a Safer Digital Future*, 17.

[110] European Commission. *Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition*.

[111] European Data Protection Supervisor (EDPS). *Leading by Example - EDPS 2015-2019 - Executive Summary*, 3.

[112] H.R.4978 - Online Privacy Act of 2019, 2019.

recommends in its Opinion on the "ePrivacy Regulation" that it should "impose an obligation on hardware and software providers to implement default settings that protect end users' devices against any unauthorised access to or storage of information on their devices."[113] While the concept of "privacy-by-design" is certainly not unique to EU discourse, it is far more consistent than in US discourse, and there are more examples of relatively specific policy recommendations such as the one mentioned above. Much like the role of the EU Charter in standardizing the rights-based discourse that pervades nearly every EU policy text, the consistency of policies like "privacy-by-design" or "data protection by design" can be traced to the GDPR, in this case Article 25(1).[114] Furthermore, the fact that most EU sources in this sample are actual policy papers compared to some of the more peripheral sources in the US sample suggests that "privacy-by-design" discourse is likely to be more impactful in the EU context. The existence of "parent texts" like the EU Charter and the GDPR seem to explain, at least in part, why the scores given to EU texts tend to be more concentrated compared to their US counterparts. As shown on Table III, most US sources fall somewhere between 0.2 and 0.9 while EU sources are generally concentrated between 1.2 and 1.6.

There are two notable cases worth discussing briefly before concluding this section. The first is the outlier represented as a lonely red dot well below the scores of other EU sources on Table III. This text is the EDPS Strategy paper for 2015-2019.[115] The most interesting thing about this text is its score which was earned because it simply falls short of the standard of collectivization established in other texts including its

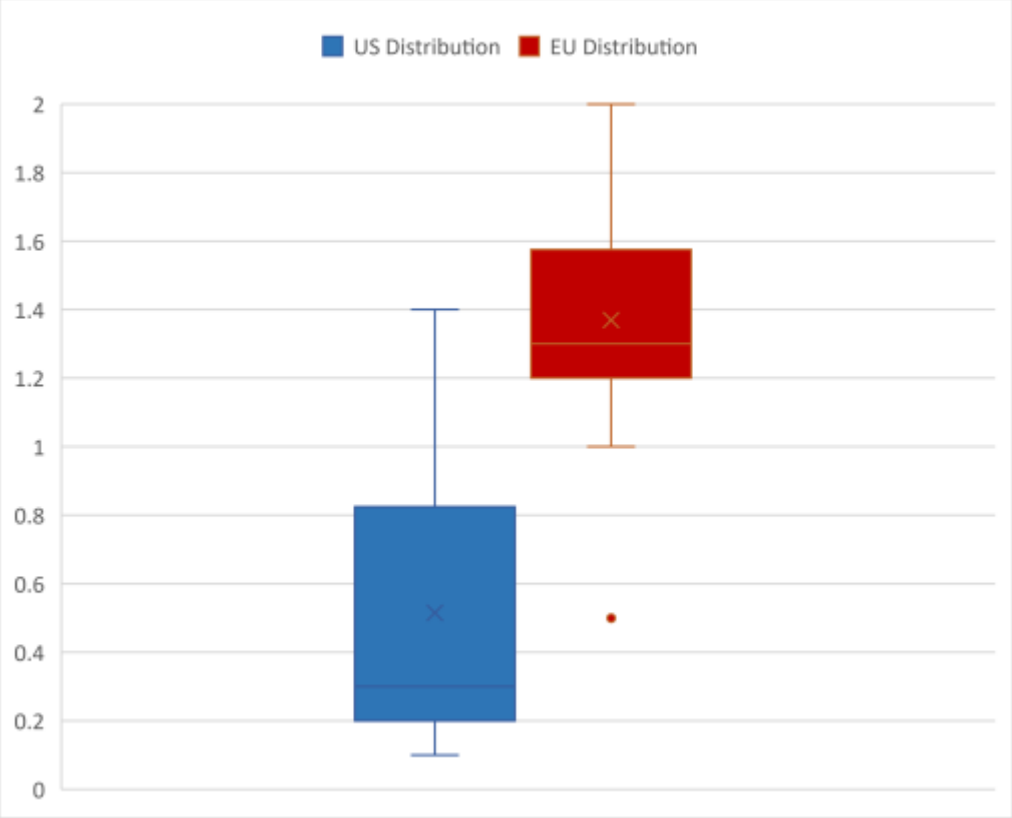
[113] European Data Protection Supervisor (EDPS). *EDPS Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*, 19.
[114] "Official Legal Text." General Data Protection Regulation (GDPR).
[115] European Data Protection Supervisor (EDPS). *The EDPS Strategy 2015-2019*.

predecessor released only two years earlier. Since it was released in 2015, prior to the GDPR, it is reasonable to say that it did not benefit from the standardizing effect of this key piece of EU data protection policy. Other than that, it does not offer anything that warrants further discussion. The second case, which is clearly more interesting, is the EDPS Strategy paper for 2020-2024. Earning a perfect score of 2.0, this text serves as the quintessential example of collectivized digital privacy discourse. As mentioned already, an individualized notion will always be at the heart of data protection, so the presence of mild or even strong individualized privacy discourse doesn't preclude a high score on this scale. Furthermore, one could easily imagine an even more collectivized text, but only two other policy texts even came near this one, so it is well deserving of being the ceiling for the scale used in this analysis. The *EDPS Strategy 2020-2024* is the text most closely aligned with the arguments of the privacy literature. Alongside the consistent reference to digital privacy as a fundamental human right and the importance of data protection for the health of democratic society, the parts of this text that discuss user control consent are also supported by the argument that these measures are insufficient, and that individuals should not bear "the burden of proof […] to understand risks and take action."[116] To illustrate further, it states: "Where the digital environment becomes more complex, responsibility falls on controllers and enforcers to avoid any data practices that harm the rights or interests of the individuals concerned."[117] That said, EU discourse generally still focuses strongly on an individualized approach, which is consistent with Bietti's evaluation of the GDPR discussed in the literature review section. This is why most EU sources still fall some distance short of the ideal 2.0 assigned to the

[116] European Data Protection Supervisor (EDPS). *The EDPS Strategy 2020-2024*, 19.
[117] Ibid.

EDPS Strategy 2020-2024 text. This paper does not dispute this fact, but this analysis has shown that there are a number of reasons why EU discourse on digital privacy is considerably more collectivized compared to the US.

Table III.



Implications for Transatlantic Relations

The pressure in recent years for greater federal data protection in the US is good news for the potential convergence of US and EU policy regimes. However, the failure of the flurry of legislative proposals to produce even a single significant new set of laws over the last few years suggests that it will take many years before this pressure is materialized

into concrete policy. So, what can be expected in the short term? Both the US and the EU emphasize the importance of having a consistent set of data protection regulations, so they will certainly be incentivized to compromise in order to have a more effective regulatory framework for transatlantic data processing. To start, both US and EU policymakers are likely to agree that cooperating on improving and standardizing the individualized approach to privacy protection. However, the greater degree of collectivization in EU discourse on digital privacy described in this paper may prove to be a source of contention in transatlantic relations on the subject, particularly considering the EU's explicitly stated interest in promoting its values through its foreign policy.[118] For example, the EDPS was clear in its 2016 Opinion on the draft EU-Canada PNR agreement that the rights guaranteed to EU citizens by the EU Charter would have to remain the minimum standard in any policy agreed with a non-EU entity. In reference to Article 8, the right to the protection of personal data, the text states: "An international agreement that governs data transfers cannot lower the level of protection of that fundamental right."[119] While this analysis considers the notion of a fundamental right to be a significant part of policy discourse on digital privacy, the discursive divide between a fundamental and a consumer right, for example, may be less impactful on actual policy outcomes than the results of the analysis suggest. To elaborate, EU policymakers could rely on a loose definition of what constitutes an adequate level of protection under the EU Charter to facilitate the negotiation of international agreements. Some degree of flexibility

[118] "Foreign and Security Policy." European Union, March 11, 2021. https://europa.eu/european-union/topics/foreign-security-policy_en#:~:text=The%20EU%27s%20joint%20foreign%20and,in%20the%20EU%27s%20international%20role.

[119] European Data Protection Supervisor (EDPS). *EDPS Pleading at the Hearing of the Court of Justice, EU-Canada PNR Agreement*, 2.

is to be expected, but the lack of a federal data protection agency in the US may constitute an acute roadblock to cooperation with the EU. In the same text on EU-Canada PNR negotiations discussed earlier, the EDPS states the following: “Article 8(3) of the Charter requires that processing be subject to control by an independent supervisory authority, which according to this Court is an essential component of the right to the protection of personal data.”[120] Unless US policymakers can make considerable headway on this issue, which from an EU perspective appears to represent the minimum standard for adequate data protection, then transatlantic cooperation on data protection will remain limited to the bear minimum required to satisfy the economic and humanitarian interests of both actors.

[120] Ibid., 10.

Conclusion

Through an analysis of forty policy texts from the US and the EU, this paper finds that EU discourse tends to collectivize the concept of digital privacy to a significantly higher degree than in the US. The dominance of both consumer-oriented language and a user-centric approach to data protection suggests that US policy discourse on data protection is dominated by an economic focus which restricts the collectivization of digital privacy in that context. On the other hand, EU policy discourse is framed by a human rights approach which enables and encourages a broader, more collectivized approach to data protection. Even though individualized policy remains the central component, EU policy discourse, and, by extension, policy itself, places a greater part of the burden on data collectors and legislators to protect the rights of individuals. While US discourse is disparate and remains stuck on baseline issues, the inevitable result of legislative deadlock, EU policymakers are operating within a more developed and concentrated discursive space. Furthermore, the most recent EDPS strategy paper shows how EU discourse is constantly pushing the boundary of what is considered adequate data protection, and it seems increasingly unlikely that the US data protection regime will be able to converge with EU standards any time soon. These discursive differences illustrate the gulf in policy which may prove to be a serious barrier to meaningful cooperation on data protection between these two actors.

In closing, how could this research be expanded upon? Due to the relatively short length of this paper, it has taken the mid-road between a quantitative content analysis with a large sample and a qualitative discourse analysis. Naturally, this compromise leaves a considerable amount of work to be done in either direction. On the content

analysis side, future research could address the weakness of the grading scale by developing one that allows for a more methodical analysis, ideally applied to a larger number of cases. Conversely, the various discursive elements could be explored in greater depth, perhaps to provide a clearer picture of the factors behind discourse and policy.

Bibliography

"CDT's Federal Baseline Privacy Legislation Discussion Draft." Center for Democracy and Technology, July 20, 2020. https://cdt.org/insights/cdts-federal-baseline-privacy-legislation-discussion-draft/.

"Foreign and Security Policy." European Union, March 11, 2021. https://europa.eu/european-union/topics/foreign-security-policy_en#:~:text=The%20EU%27s%20joint%20foreign%20and,in%20the%20EU%27s%20international%20role.

"Official Legal Text." General Data Protection Regulation (GDPR), September 2, 2019. https://gdpr-info.eu/.

"Principles for Privacy Legislation." New America, November 13, 2018. https://www.newamerica.org/oti/press-releases/principles-privacy-legislation/.

Bennett, Colin J. "In Defense of Privacy: The Concept and the Regime." S*urveillance & Society* 8, no. 4 (2011): 485–96. https://doi.org/10.24908/ss.v8i4.4184.

Bietti, Elettra. *The Discourse of Control and Consent over Data in EU Data Protection Law and Beyond*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2001. https://www.hoover.org/research/discourse-control-and-consent-over-data-eu-data-protection-law-and-beyond

Brenkert, George G. "Business Ethics and Human Rights: An Overview." *Business and Human Rights Journal* 1, no. 2 (2016): 277–306. https://doi.org/10.1017/bhj.2016.1.

Brown, Michael, and Carrie Klein. “Whose Data? Which Rights? Whose Power? A Policy Discourse Analysis of Student Privacy Policy Documents.” *The Journal of Higher Education* 91, no. 7 (2020): 1149–78. https://doi.org/10.1080/00221546.2020.1770045.

Byford, Katrin Schatz. “Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment.” *Rutgers Computer and Technology Law Journal* 24, no. 1 (1998): 1–74.

Council of the European Union. *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*. 2011. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52011PC0032

Draper, Nora A. “From Privacy Pragmatist to Privacy Resigned: Challenging Narratives of Rational Choice in Digital Privacy Debates.” *Policy & Internet* 9, no. 2 (2016): 232–51. https://doi.org/10.1002/poi3.142.

European Commission. *Commission Staff Working Document - Executive Summary of the Ex-post REFIT evaluation of the ePrivacy Directive*. Brussels: 2017. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications

European Commission. *Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the*

General Data Protection Regulation. Brussels: 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264

European Commission. *Communication from the Commission to the European Parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond – taking stock*. Brussels: 2019. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2019:0374:FIN

European Commission. *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*. Brussels: 2017. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications

European Data Protection Board (EDPB). *Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan*. https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-282018-regarding-european-commission-draft_en

European Data Protection Board (EDPB). *Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive*, 2021. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_en

European Data Protection Supervisor (EDPS). *Annual Report 2016 - Executive Summary.* Luxembourg: Publications Office of the European Union, 2017. https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2016-annual-report-state-privacy-2017-edps_en

European Data Protection Supervisor (EDPS). *Annual Report 2017 - Executive Summary.* Luxembourg: Publications Office of the European Union, 2018. https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2017-annual-report-data-protection-and-privacy_en

European Data Protection Supervisor (EDPS). *Annual Report 2018 - Executive Summary.* Luxembourg: Publications Office of the European Union, 2019. https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2018-annual-report-new-era-data-protection_en

European Data Protection Supervisor (EDPS). *Annual Report 2020 - Executive Summary.* 2021. https://edps.europa.eu/data-protection/our-work/publications/annual-reports/annual-report-2020_en

European Data Protection Supervisor (EDPS). *EDPB-EDPS Joint Opinion on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*. 2021. https://edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-opinion-proposal-regulation-european_en.

European Data Protection Supervisor (EDPS). *EDPS Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*.

2017. https://edps.europa.eu/data-protection/our-work/publications/opinions/eprivacy-regulation_en

European Data Protection Supervisor (EDPS). *EDPS Pleading at the Hearing of the Court of Justice, EU-Canada PNR Agreement*. 2016. https://edps.europa.eu/data-protection/our-work/publications/court-cases/edps-pleading-hearing-court-justice-eu-canada-pnr_en.

European Data Protection Supervisor (EDPS). *Leading by Example - EDPS 2015-2019 - Executive Summary*. Luxembourg: Publications Office of the European Union: 2019. https://op.europa.eu/webpub/edps/edps-2015-2019-executive-summary/en/

European Data Protection Supervisor (EDPS). *Promoting a new culture of data protection: Annual Management plan 2019 – Summary*. Luxembourg: Publications Office of the European Union: 2019. https://edps.europa.eu/press-publications/publications/strategy_en

European Data Protection Supervisor (EDPS). *Strategy 2013-2014: Towards excellence in data protection*. Luxembourg: Publications Office of the European Union: 2012. https://edps.europa.eu/data-protection/our-work/publications/strategy/strategy-2013-2014_en

European Data Protection Supervisor (EDPS). *The EDPS Strategy 2015-2019: Leading by Example*. Luxembourg: Publications Office of the European Union: 2015. https://edps.europa.eu/data-protection/our-work/publications/strategy/strategy-2015-2019_en

European Data Protection Supervisor (EDPS). *The EDPS Strategy 2020-2024: Shaping a Safer Digital Future*. 2020. https://edps.europa.eu/data-protection/our-work/publications/strategy/edps-strategy-2020-2024-shaping-safer-digital-future_en

González Fuster, Gloria. "The Emergence of Personal Data Protection as a Fundamental Right of the EU." *Law Governance and Technology Series* 16 (2014): 1–272.

Group, Global Legal. "Data Protection 2020: Laws and Regulations: USA: ICLG." International Comparative Legal Guides International Business Reports. Global Legal Group. Accessed April 5, 2021. https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

H.R.4978 - Online Privacy Act of 2019. Bill introduced to the 116th U.S. Congress (2019).

Kennedy P. "Individualization and the Cultures of Capitalism." In: *Vampire Capitalism*. Palgrave Macmillan, London, 2017. https://doi.org/10.1057/978-1-137-55266-2_6

Peppet, Scott R. "Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future." *Northwestern University Law Review*, 2011, 1–52.

Purtova, Nadezhda. "Property Rights in Personal Data: Learning from the American Discourse." *Computer Law & Security Review* 25, no. 6 (2009): 507–21. https://doi.org/10.1016/j.clsr.2009.09.004.

S.1214 - Privacy Bill of Rights Act. Bill introduced to the 116th U.S. Congress (2019).

S.2968 - Consumer Online Privacy Rights Act. Bill introduced to the 116th U.S. Congress (2019).

S.3300 - Data Protection Act of 2020. Bill introduced to the 116th U.S. Congress (2020).

Schwartz, Paul M. “Internet Privacy and the State.” *Connecticut Law Review* 32, no. 3 (2000): 815–60.

Tzanou, Maria. “Data Protection as a Fundamental Right next to Privacy? 'Reconstructing' a Not so New Right.” *International Data Privacy Law* 3, no. 2 (2013): 88–99. https://doi.org/10.1093/idpl/ipt004.

U.S. Congressional Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce. *Opening Statement*. Chairman Frank Pallone, Jr. Hearing on “Oversight of the Federal Trade Commission: Strengthening Protections for Americans’ Privacy and Data Security.” Washington D.C.: 2019. https://energycommerce.house.gov/newsroom/press-releases/pallone-remarks-at-ftc-oversight-hearing-0

U.S. Congressional Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce. *Opening Statement*. Chair Jan Schakowsky. Hearing on “Oversight of the Federal Trade Commission: Strengthening Protections for Americans’ Privacy and Data Security.” Washington D.C.: 2019. https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/2019.5.8.SCHAKOWSKY.%20FTC%20Oversight%20Hearing.CPC__0.pdf

U.S. Federal Trade Commission*. Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases*. Maureen K. Ohlhausen. Washington D.C.:

2010. https://www.ftc.gov/public-statements/2017/09/painting-privacy-landscape-informational-injury-ftc-privacy-data-security

U.S. Federal Trade Commission. *Prepared Statement of the Federal Trade Commission On The State of Online Consumer Privacy*. Washington D.C.: 2019. https://www.ftc.gov/public-statements/2011/03/prepared-statement-federal-trade-commission-state-online-consumer-privacy

U.S. Federal Trade Commission. *Prepared Statement of the Federal Trade Commission: Oversight of the Federal Trade Commission Before the Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce, United States House of Representatives*. Washington D.C.: 2019. https://energycommerce.house.gov/committee-activity/hearings/hearing-on-oversight-of-the-federal-trade-commission-strengthening

U.S. Senate Committee of Commerce, Science, and Transportation. *The State of Online Privacy and Data Security*. Ranking Member Maria Cantwell. Washington D.C.: 2010. https://www.cantwell.senate.gov/imo/media/doc/The%20State%20of%20Online%20Privacy%20and%20Data%20Security.pdf

U.S. Senate Committee on Commerce, Science, and Transportation. *Discussion Draft of the United States Consumer Data Privacy Act*. Chairman Roger Wicker. Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/chairman-wicker-s-discussion-draft-the-united-states-consumer-data-privacy-act

U.S. Senate Committee on Commerce, Science, and Transportation. *Majority Statement*. Chairman Roger Wicker. Hearing on “Examining Legislative Proposals to Protect Consumer Data Privacy.” Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

U.S. Senate Committee on Commerce, Science, and Transportation. *Minority Statement*. Ranking Member Maria Cantwell. Hearing on “Examining Legislative Proposals to Protect Consumer Data Privacy.” Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

U.S. Senate Committee on Commerce, Science, and Transportation. *Written Testimony*. Julie Brill. Hearing on “Examining Legislative Proposals to Protect Consumer Data Privacy.” Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

U.S. Senate Committee on Commerce, Science, and Transportation. *Written Testimony*. Maureen Ohlhausen. Hearing on “Examining Legislative Proposals to Protect Consumer Data Privacy.” Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

U.S. Senate Committee on Commerce, Science, and Transportation. *Written Testimony*. Laura Moy. Hearing on “Examining Legislative Proposals to Protect Consumer

Data Privacy." Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

U.S. Senate Committee on Commerce, Science, and Transportation. *Written Testimony*. Nuala O'Connor. Hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy." Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

U.S. Senate Committee on Commerce, Science, and Transportation. *Written Testimony*. Michelle Richardson. Hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy." Washington D.C.: 2019. https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy

Westin, Alan F*. Privacy and Freedom*. New York: Atheneum, 1970.