A NEW REGULATORY DAWN FOR ONLINE CONSUMERS IN THE UNITED STATES

Dr Ann Kristin Glenster
Senior Advisor on Technology Governance and Law
October 2022

MINDEROO CENTRE FOR TECHNOLOGY & DEMOCRACY

October 2022

This report is authored by Dr Ann Kristin Glenster, Senior Advisor on Technology Governance and Law, Minderoo Centre for Technology and Democracy, University of Cambridge.

Minderoo Centre for Technology and Democracy

The Minderoo Centre for Technology and Democracy is an independent team of academic researchers at the University of Cambridge, who are radically rethinking the power relationships between digital technologies, society and our planet.

www.mctd.ac.uk

CONTENTS

EXECUTIVE SUMMARY AND RECOMMENDATIONS

This report is the University of Cambridge Minderoo Centre for Technology and Democracy's response to the Federal Trade Commission's ('FTC') request for submissions 'Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking Commission File No. R111004' ('ANPR submissions'). Our recommendations focus on the need to adopt mandatory data processing principles and consumer consent.

We situate our advice in the context of the historical role the FTC has played as a de facto privacy regulator, and how the rise of commercial surveillance means that new trade regulation rules are urgently needed. The implications of endemic commercial surveillance are far-reaching. Not only has the hoarding and monetization of personal data undermined the belief that individuals can have privacy online, it has also had negative effects on consumer freedoms and their trust in the digital economy. The result is a worrying loss of personal autonomy and consumers' ability to participate in the market. The deleterious knock-on effect is diminishing consumer confidence in the digital economy, which is part of a larger picture of trust being eroded in civil society.

Our key recommendations are:

1. Mandatory Data Processing Principles

    - The FTC should adopt new trade regulation rules which include a mandatory obligation placed on companies to adhere to the transparency, data minimization, purpose limitation, and duration limitation principles in relation to all processing of consumer data.

2. Consumer Consent

    - The FTC should adopt new trade regulation rules governing the use of consumer consent by companies online.
    - Consent should be mandatory in some instances, and whenever used, it should conform to standards similar to those in EU law, including the right to withdrawal consent and the stipulations that consent must be informed.
    - Consent should not be used in situations where the consumer cannot reasonably consent, such as to profiling based on personal data harvested without the consumer's knowledge or understanding.
    - Receiving access to goods and services should not be contingent on consent to the processing of personal data unless strictly necessary for the performance of contract or the delivery of those goods or services.

3. Definition of Personal Data

    - The FTC should adopt a definition of personal data that clarifies which data is covered by the data processing principles and consumer consent
    - The definition of personal data should be wider than the definition of 'private' data or 'sensitive' data
    - The definition of personal data should be technologically neutral

The submission has three parts: (i) this report contextualizing our advice, (ii) specific answers to selected questions of the FTC's ANPR submission request, and (iii) a comparative overview of data processing principles. Our recommendations draw on a comparative analysis of the European data protection regime. We are mindful that while lessons can be learned from the European Union, any rules imported must be adapted to the specific American context.

INTRODUCTION

New trade regulation rules to protect American consumers in the digital economy are long overdue. As is well established, since its first foray into Internet regulation with GeoCities[1], the FTC has taken on the role as the de facto privacy regulator of the United States ('U.S.').[2] Section 5 of the Federal Trade Commission Act of 1914 ('FTC Act') tasks the FTC with preventing and redressing 'unfair and deceptive acts and practices.[3] It is important to understand the scope of this mandate, and how it sits in the federal regulatory landscape when considering whether the FTC should, and if so how, promulgate new trade regulation rules to protect consumers online.[4]

The signal that new trade regulation rules are being considered marks a potential watershed in U.S. regulation of commercial surveillance in the digital economy. It also comes at a time when calls for rules have grown to a crescendo,[5] which risks attracting expectations that the FTC can promulgate rules which would reach wider that its mandate allows, or that it can address a plethora of issues beyond its scope. In assessing

[1] Geocities, Docket No. C-3850, February 5, 1999.
[2] Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Columbia L.J. 583, 583-676 (2014). Kenneth A. Bamberger and Deirdre K. Mulligan, Privacy on the Ground: Driving Corporate Behaviour in the United States and Europe (The MIT Press 2015), 69.
[3] FTC Act of 1914, 15 U.S.C. §§ 41-58.
[4] Section 18 of the FTC Act affords the FTC this power.
[5] e.g., Mark MacCarthy, 'Why the FTC should proceed with a privacy rulemaking', Brookings Institute, June 29, 2022 https://www.brookings.edu/blog/techtank/2022/06/29/why-the-ftc-should-proceed-with-a-privacy-rulemaking/ accessed September 21, 2022; Epic.org., What the FTC Could Be Doing (But Isn't) To Protect Privacy, June 2021; Robert Gellman, 'Can Consumers Trust the FTC to Protect Their Privacy?', ACLU, October 25, 2016 https://www.aclu.org/news/privacy-technology/can-consumers-trust-ftc-protect-their-privacy accessed September 21, 2022.

proposals for new trade regulation rules, it is therefore important to recognize the scope of the FTC's remit and what the FTC, within the law and with its finite resources, can realistically achieve. Bearing that in mind, new trade regulation rules present an opportunity for the FTC to keep American consumers safe and to stimulate the U.S. economy by fostering consumer trust and ensuring fairness in the digital marketplace.

Applying a comparative lens, this report draws on the experiences of the EU data protection regime. However, we note that this regime cannot be simply duplicated for the U.S. We are also skeptical to placing too much emphasis on consumers' actions: In many cases consumers cannot and should not carry the responsibility for what the tech industry does with consumer data. As such, our advice attempts to strike the right balance between consumer empowerment and holding the tech industry to account.

COMMERCIAL SURVEILLANCE

The growth of the U.S. technology industry has been a boon for the digital economy. It has brought phenomenal benefits to people, business, and government on an unprecedented scale. This achievement has also come with costs, chief among these the sacrifice of online privacy of U.S. consumers. The implications are far-reaching. Not only has the hoarding and monetization of personal data undermined the belief that individuals can have privacy online, it has also

had negative effects on consumer freedoms and their trust in the digital economy.

Over the last twenty years, behemoth technology companies have built commercial empires from harvesting consumer data in the U.S. and abroad. These empires could not have been built had they been subjected to more stringent rules regarding the online privacy of their customers. These empires are further built on network effects, whereby customers are locked into networks – for example 'everyone' is on a social media platform which makes it worthless to move to another platform – where the benefits outrank the perceived cost. Increasingly, it has become unfeasible for consumers to leave or switch online service providers, and some social platforms have even taken on functions comparable to utilities.[6] The notion that consumers are free to choose the 'privacy package' that best suits them in this unregulated environment has therefore to a large extent unraveled.

The absence of basic federal protection of online privacy means that commercial actors are free to gather data on consumers and use that data for a range of purposes with little compunction. Automated algorithms use personal data to determine the types of news, entertainment, and advertisements a person will encounter in the digital space. Personal data is used for credit-scoring, profiling, and a host of other discriminatory practices. While not always overtly illegal, these forms of discrimination contribute to the further entrenchment of inequalities in society. For example, research has demonstrated cases

[6] For example, the professional social media platform LinkedIn.

of black social media users being shown advertisements for janitorial jobs but not office vacancies requiring a college degree.[7] As personal data is used to personalize the commercial online environment, consumers are presented with fewer market choices. While the long-term consequences of routinized commercial surveillance are yet unknown, it is certain that American consumers have very little influence or say over how their online identities or profiles are generated or scored. The result is a worrying loss of personal autonomy and consumers' ability to participate in the market. The deleterious knock-on effect is diminishing consumer confidence in the digital economy, which is part of a larger picture of trust being eroded in civil society.

The time is therefore ripe for the FTC to promulgate new trade regulation rules which will empower consumers, hold the tech industry to account, and thereby foster consumer confidence in the digital economy. This is a pressing and urgent matter for the digital economy to continue to thrive for the benefit of all of society.

CONSUMER PRIVACY

The FTC is soliciting submissions on whether it should promulgate new trade regulation rules to protect consumer privacy in the context of routinized digital commercial surveillance. This formulation raises several thorny questions, notably as will be seen when compared to the

[7] Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Alexandra Korolova, Alan Mislove, Aaron Rieke, Discrimination through optimisation: How Facebook's ad delivery can lead to skewed outcomes, arXiv:1904.0209505, Proceedings of the ACM on Human-Computer Interaction 2019.

European data protection regime, of the distinction between 'privacy' and 'data.'

Background to Consumer Privacy in the Context of the FTC

The issue of consumer privacy has a long history in the U.S., which is tied to the American understanding of privacy.

The origins of privacy are habitually traced to Warren and Brandeis' seminal article in the Harvard Law Review, published in 1890, as a reaction against new camera technology, rise of paparazzi photographers, and burgeoning 'yellow journalism.'[8] Warren and Brandeis famously defined the 'right to privacy' as 'the right to be let alone.'[9] From this flows the notion of privacy as a matter of having the right to control the disclosure of certain information. This conceptualization of privacy as the right to keep information 'hidden' or 'secret' is echoed in Prosser's four privacy torts, established in another academic article published in 1960.[10] Warren and Brandeis' seminal article and the privacy torts form the foundation for privacy protection in the commercial sphere in U.S. law.[11] The idea that privacy as a right to keep information secret was also central to the warnings against the

[8] Samuel D. Warren, Louis Brandeis, The Right to Privacy, 4(5) Harvard L.R. 193, 193-220 (1890).
[9] ibid.
[10] William L. Prosser, Privacy, 48 Calf. L. Rev. 383, 383 (1960). Prosser listed the four privacy torts as: (i)intrusion on a person's seclusion or solitude; (ii) public disclosure of embarrassing private facts about a person; (iii) publicity that places a person in a false light in the public eye; and (iv) appropriation, for the defendant's advantage, of the person's name or likeness.
[11] This is different from the protection afforded under the Constitutional Amendments concerning privacy intrusions by government (e.g., in Griswold v. Connecticut, 381 U.S. 479, S. Ct. 1678, 14 L.Ed.2d 520; Eisenstadt v. Baird, 405 U.S. 438 (1972); Lawrence v. Texas (02-102) 539 U.S. 598 (2003).

new world of electronic data processing and databanks emerging in the 1960s and 1970s.[12]

Ever since the 1973 Department of Health, Education and Welfare Advisory Committee on Automated Data Systems report ('HEW report') recommended the enactment of federal legislation to give effect to the Fair Information Practices (FIPs),[13] policymakers and legislators have debated whether to make privacy protection part of federal statutory law. To recall history, U.S. Congress did not fully follow the 1973 recommendations, and only partially adopted the FIPs in federal law in the landmark Privacy Act of 1974,[14] which only applies to government and public authorities' processing of personal information. Several federal statues were later enacted,[15] but these only pertained to specific industry sectors, giving rise to the description of the American model of privacy protection as piecemeal and ad hoc.[16] It also meant that there is no federal regulation of the commercial treatment of consumer data beyond the guidance, practices, and caselaw of the FTC.

Thus, when calling on the FTC to formally adopt the role federal online privacy regulator, proponents of such suggestions also call for the FTC to fill a statutory gap Congress has left to widen for decades.[17]

---

[12] Notably Alan F. Westin, Privacy and Freedom (Atheneum 1970); Arthur R. Miller, The Assault on Privacy: Computers, Data Banks, and Dossiers (The University Press 1970).
[13] U.S. Department of Health, Education, and Welfare ('HEW'), Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems (July 1973).
[14] The Privacy Act of 1974, as amended, 5 U.S.C. § 552a.
[15] e.g., Fair Credit Reporting Act of 1970, 6 U.S.C. § 142(a)(2); Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. 106-191; Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232g.
[16] David L. Baumer, Julia B. Earp, J.C. Pointdexter, Internet privacy law: a comparison between the United States and the European Union, 23(5) Computers & Security 400, 400-412 (2004).
[17] Epic.org., What the FTC Could Be Doing (But Isn't) To Protect Privacy, June 2021

THE FTC'S ONLINE PRIVACY PRACTICES

The FTC has taken a narrow approach to its role as a de facto privacy regulator based on the wording of Section 5 of the FTC Act. As FTC caselaw has considered what would constitute unfair or deceptive privacy policies, the more foundational issue of whether consumers should have a reasonable expectation to privacy has been left to guidance and encouragement of industry practices under the guise of industry self-regulation.[18]

However, there is no uniform definition of the concept of privacy. In his taxonomy, legal scholar Daniel J. Solove applied Wittgenstein's idea of family resemblance to find that privacy is a set of related concepts.[19] Over the decades, other scholars have added new forms of privacy to his taxonomy, including informational privacy, decisional privacy, and intellectual privacy, to mention a few.[20] Still, the core notion of privacy remains the right to control the disclosure of certain types of personal information.

The starting point for the FTC's concept of privacy is therefore the protection of some types of information whose disclosure should be controlled. This is different from the notion that the use of all personal information should be regulated, or that the regulatory rules should extend to the way personal information is used once it has been disclosed. The traditional concept of privacy thus poses some key

[18] Federal Trade Commission, Privacy Online: A Report to Congress (June 1998).
[19] Daniel J. Solove, Conceptualizing Privacy, 90 Cal. L. Rev. 1087 (2002).
[20] e.g., Neil Richards, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (Oxford University Press 2015).

challenges to the FTC if it decides to adopt new trade regulation rules governing commercial surveillance. Digital commercial surveillance is about data, not individuals. While conflated in mainstream literature and discourse, surveillance of a person and surveillance of personal data are two different things.

Adopting new trade regulation rules governing routinized commercial surveillance would necessitate enlarging the scope of privacy from personal information that individuals should have a right to keep hidden, to all personal data. This would represent a seismic shift in the American understanding of privacy. However, there are no impediments to the FTC enlarging its regulatory framework to cover all personal data when that data is subjected to unfair or deceptive acts and practices, which routinized commercial surveillance could be seen to do. Indeed, in the decades since GeoCities, the FTC has enforced online privacy concerning the use of personal information in the context of privacy policies, regardless of whether that information was 'private' or already disclosed.

Addressing issues of deceptive practices in the commercial online space has been easier than 'fairness' as deception can be evidence by either false or misleading information about how customers' privacy will be handled or omissions to inform customers of the same. In contrast, issues of fairness have been more difficult to pin down,[21] largely

[21] Chris Jay Hoofnagle, Federal Trade Commission: Privacy Law and Policy (Cambridge University Press 2016).

because any intervention by the FTC could quickly be seen as interference with free competition.[22]

While the FTC has a role to play in ensuring fairness between different market actors, it cannot impose conditions onto these market actors when such conditions would (a) place a burden on (especially small businesses) to adopt privacy policies at disproportionate cost, or (b) eradicate the competitive advantage of companies who have made strong privacy policies integral to their commercial USP.[23] The claim of some academics that privacy is no more than a product feature has thus prevailed for decades.[24] Ultimately, it has been left to the consumer to choose the 'privacy package' offered by the service or product provider which suits them best.

Consequently, FTC's enforcement action has focused not on whether consumers have been afforded online privacy, but whether companies have adhered to the promises made to consumers in their privacy policies.[25] When companies responded by either avoiding having privacy policies or making these policies so long and dressed in such legalese that they would be useless to consumers, the FTC developed new industry standards. These new standards included requirements of privacy policies, and that these were made accessible, legible, and

[22] e.g., Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress (2000): Dissenting statement by Commissioner Orson Swindle, pp. 15-16.
[23] Apple is a good example.
[24] Richard A. Epstein, Law and Economics: Its Glorious Past and Cloudy Future, 64 U. of Chicago L. Rev. 1167 (1997); Richard A. Posner, The Economics of Justice (Harvard University Press 1983); Steven Shavell, Foundations of Economic Analysis of Law (The Belknap Press of Harvard University Press 2004); Richard A. Posner, Gary Becker's Contribution to Law and Economics, 22(2) The J. of L. Studies 211 (1993).
[25] e.g., In re Google Inc., FTC File No. 102 3136, No. C-4336 (October 13, 2011); In re Facebook Inc., FTC File No. 092 3184, No. C-4365 (July 27, 2012); Microsoft Corporation, Docket No. C-4069 (August 8, 2002) (Agreement Containing Consent Order); Epic Marketplace Inc., Docket No. C-4389 (March 13, 2013).

understandable to the average consumer.[26] However, there is a limitation to how far the FTC's regulatory innovations and adaptations can evolve without further promulgation of dedicated privacy rules.

This means that the FTC's approach to consumer privacy has languished for more than two decades, during which time commercial treatment of consumer data has undergone a radical paradigm shift. In fairness, the FTC has made incremental adjustments along the way. However, no initiative has been adopted that has come near to addressing the fundamental structural changes that has taken place between commercial actors and consumers regarding the way personal data is harvested, generated, and commodified in the digital economy.

MANDATORY DATA PROCESSING PRINCIPLES?

In its ANPR submissions call, the FTC asks if it should promulgate new trade regulation rules which would impose mandatory transparency, data minimization, purpose limitation, and duration limitation requirements on businesses' processing of consumer data. These requirements relate to the European Union's ('EU') obligatory data processing principles set out in Article 5 of the General Data Protection Regulation ('GDPR'),[27] which constitutes the EU's comprehensive data protection regime. This question is therefore in part a question of whether the U.S. should import a set of rules from a foreign jurisdiction.

[26] In the Matter of Vision I Properties, LLC, d/b/a Cartmanger International, Docket No. C-4135, April 19, 2005.
[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119.

However, the data processing principles are not entirely foreign to the U.S. as they relate to the Fair Information Practices (FIPs), which were conceived in the HEW report in 1973.[28] The original five FIPs were:

1. There must be no personal data record-keeping system whose very existence is kept secret.

2. There must be a way for a person to find out what information about the person is in a record and how it is used.

3. There must be a way for a person to prevent information about the person that was obtained for one purpose being used or made available for other purposes without the person's consent.

4. There must be a way for a person to correct or amend a record of identifiable information about the person.

5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must take precaution to prevent misuse of the data.

The FIPs already play a noticeable role in the FTC's oversight of the digital economy in the guise of the Fair Information Practice Principles ('FIPPs'), which were introduced by the FTC under its Notice, Choice, Access and Security framework in 1998.[29]

The five FIPPs are:

1. Notice and Awareness

2. Choice and Consent

3. Access and Participation

[28] HEW Report (supra note 13).
[29] FTC (supra note 18). Federal Trade Commission, Fair Information Practices Principles: A Practice Statement (1998). The Practice Statement was reissued in 2000.

4. Integrity and security

5. Enforcement

Returning to the conception of the FIPs, the HEW report strongly recommended that these be made mandatory through the enactment of federal legislation. However, when the HEW report was followed only three years later by the 1977 Privacy Protection Study Commission ('PPSC'), its report recommended that the FIPs stay voluntary.[30] When the FTC adopted the FIPPs in 1998, they were part of an industry self-regulated scheme.[31] While adding the enforcement principle, the FIPPs could still only be enforced with the cooperation of industry. In short, unlike the intention behind the FIPs, the FIPPs are guiding principles rather than reliable enforceable rules. In 2000, the FTC recognized that the reliance on voluntary compliance with the FIPPs was failing, and recommended they become mandatory through Congressional enactment.[32] This recommendation was not followed by Congress, partially for reasons which will be visited in the conclusion of this report.

The original FIPs included a principle which went some way to embody what the FTC now seems to suggest would be the function of the transparency, data minimization, purpose limitation, and storage limitation principles. As mentioned, the third FIP stated that, 'There must be a way for a person to prevent information about the person that was obtained for one purpose being used or made available for other purposes without the person's consent.' The third FIP was clearly

[30] Privacy Protection Study Commission ('PPSC'), Personal Privacy in an Information Society (July 1977).
[31] FTC (supra note 18).
[32] FTC (supra note 22).

intended to provide individuals with some control. While not outright giving individuals the right to veto processing, it nevertheless gave them the right to impose restrictions on processing beyond the initial purpose. This intention was not carried forward into the FIPPs.

While the FIPPs include a principle called Access and Participation, the guidance issued by the FTC makes it clear that this principle does not confer on individuals any right to control the processing of their personal data. It only affords individuals the right to view what personal information an entity is holding and to correct any inaccurate information in those files. This can hardly be said to empower consumers to control or influence the way their personal information is used in the context of commercial surveillance.

As such, despite their names, the FIPPs represent a shift away from empowering consumers to holding personal data processing entities accountable. It also illustrates the tension that runs through the history of personal data regulation, on either side of the Atlantic, of how to 'level the playing field' between consumers and companies in a world constructed from extreme information asymmetries and power imbalances. The shift towards holding companies accountable is an attempt to level this field. However, it is predicated on maintaining the fiction that consumers have 'real choice' in the digital economy. The FIPPs are thus applied to recalibrate the scales, but their success in so doing has been limited, in part because the technology has advanced at a much greater pace than the regulatory advice.[33] In any case, it must be

[33] This is the classic pacing problem. For discussion, see Meg Leta Jones, The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood, 47 Soc. Stud. Sci. 216 (2017); Meg Leta

reiterated that the FIPPs are merely advisory and do not have legally binding force.

In contrast, the European data protection principles are mandatory and must be adhered to in full. The data processing principles are set out in Article 5 GDPR as:

Article 5(1)(a) GDPR

Lawfulness, fairness and transparency: Personal data shall be, 'processed lawfully, fairly, and in a transparent manner in relation to the data subject'.

Article 5(1)(b) GDPR

Purpose limitation: Personal data shall be, 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes'.

Article 5(1)(c) GDPR

Data minimisation: Personal data shall be, 'adequate, relevant and limited in relation to the purposes for which they are processed'.

Article 5(1)(d) GDPR

Jones, Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw, 2 J. L. Tech. & Pol'y 101, 103 (2018); Lyra Bennett Moses, Agents of Change: How the Law 'Copes' With Technological Change, 20(4) Griffith L. Rev. 763, 788 (2011).

Accuracy: Personal data shall be 'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'.

Article 5(1)(e) GDPR

Storage limitation: Personal data shall be, 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subjects'.

Article 5(1)(f) GDPR

Integrity and confidentiality: Personal data shall be, 'processed in a manner that ensures appropriate security of their personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.

Article 5(2) GDPR

Accountability: 'The controller shall be responsible for, and be able to demonstrate compliance with [Article 5 GDPR]'.

The FTC is considering the principles of purpose limitation (Article 6(1)(b) GDPR), data minimization (Article 5(1)(c) GDPR), and storage limitation (Article 5(1)(e) GDPR) to be included in potential new trade regulation rules. The question for the FTC is therefore not simply whether to make the FIPs and/or the FIPPs mandatory for all commercial processing of personal information, but whether to adopt these in conjunction with or replace them with all or some of the European data processing principles.

To evaluate the implications of these choices, there is a comparative overview attached to the end of this report which explains the relationship between the three sets of principles. The overview reveals that there is an overlap between the five FIPPs and first, fourth, sixth, and seventh GDPR data processing principle. Suggestions for the adoption of mandatory data minimization, purpose limitation, and duration limitation principles cover the remaining second, third, and fifth principle in the GDPR. The FTC is also considering making transparency, which is already present in the FIPPs and mandatory under Article 5(1)(a) GDPR, a principle in any new trade regulation rules.

While instituting transparency, data minimization, purpose limitation, and duration principles as mandatory rules would be a significant improvement to the protection of consumers' data in relation to commercial surveillance, it leads to several issues. First, making these principles mandatory while the remaining FIPPs are left as voluntary would be flawed. The GDPR data processing principles effectiveness depends on their interdependency. They cannot be divided and applied

separately and still offer the level of data protection that is fundamental to the European data protection regime. Second, the adoption of mandatory data processing principles in new trade regulation rules will be undermined if their scope is left undefined. This is particularly true for the scope of consumer/personal data, as will be explained next. Third, the effectiveness of instituting data processing principles in new trade regulation rules will also depend on their technical specifications. Part of the problem with the FIPPs is that they lack technical specifications which makes them too vague to be enforceable. The expectation of technical compliance needed to give effect to the data processing principles must therefore be stated clearly in the new trade regulation rules. This includes the process for auditing technical compliance by the FTC.

Significantly, the adoption of the data processing principles of the GDPR in new trade regulation rules would also shift the U.S. regulatory approach away from privacy towards data protection, or reasons which have been outlined earlier in this report. More detailed comments on the possible adoption of the data processing principles in new trade regulation rules are appended to this report in the Q&A document on 'Collection, Use, Retention and Transfer of Consumer Data' and 'Consumer Consent' in response to the FTC's call for ANPR submissions.

Overall, our recommendation is that the FTC adopt the data processing principles as mandatory principles in new trade regulation rules and that

our advice regarding their wording, obligations regarding compliance, and oversight and auditing is also followed.

CONSUMER DATA

Key to the effectiveness of any mandatory rules governing the commercial processing of customer data is the definition of what data this covers. This is perhaps the most important lesson the FTC can take away from the GDPR. This is because the definitions of personal information or personal data is different in the two jurisdictions.

Historically, the term personal identifying/identifiable information ('PII') has been used in the U.S., while in Europe the term is 'personal data.' This difference is significant because personal data is set out in technology neutral language intended to be comprehensive and therefore forward-looking.[34] In contrast, PII is narrower and context specific. While several federal sectoral statutes and government guidance refer to PII, the term is rarely defined. Consequently, there is no uniform definition of PII in US law. The term is therefore not equally comprehensive to personal data in European law.

This matters as what consumers consider their personal data or customer data may vary significantly from what commercial entities regard as personal data. Any mandatory rules concerning the commercial processing of consumer data or personal data will be ineffective if these terms are not defined. Devising these definitions will

[34] The requirement of technology neutrality is set out in Recital 15 GDPR.

lead to questions regarding the level of pseudonymization, probabilities of re-identification, and labelling of data with signifiers which can be combined to reveal identity, including data that is kept by third parties. Without a clear definition, companies are likely to under-label or under-identify personal data, or the definition will be too broad for consumers to identify the data it covers as their own.

Enlarging the scope of the definitions to cover all consumer data that is being subjected to commercial surveillance would decouple new trade regulation rules from classic privacy doctrine. An earlier section of this report established how privacy is linked to information individuals would like to keep private because it is sensitive or may cause embarrassment. Thus, medical data or financial records are often considered private.[35] However, medical data or financial data is only a small fraction of the types of data that is garnered and commodified through ubiquitous commercial surveillance. Should the FTC choose to adopt new trade regulation rules, these cannot be limited to the protection of consumer data that is 'sensitive' or 'private' because privacy alone is no longer what is at stake.

CONSUMER CONSENT

The FTC requests submissions regarding whether new trade regulation rules should include mandatory consumer consent. This is a complex

[35] The emphasis on financial records and medical data as private is evidenced by the fact that Congress have adopted statutes that regulate their processing; e.g., FTC and HIPAA (supra note 15).

issue and again it is illuminating to consider how the EU has addressed it in the GDPR.

Before examining the GDPR and consent, it must be remembered that there is no mandatory right to consent to the processing of consumer/personal data in U.S. law. Partially this is because the data is not considered in law to 'belong' to the person it concerns,[36] and partially because it is assumed that consumers freely part with it when they enter into a bargain or 'contract' with an Internet service provider. Any regulatory rules governing consent could therefore be viewed as an interference in the key doctrines of American contract law, namely 'freedom to contract' and 'sanctity of contract.'[37] The only rules governing the use of consent beyond contract law in the U.S. are limited to the guidance provided by the FTC, specifically the FIPPs.

The FIPPs do not include a right to veto processing. The assumption is that individuals have already approved the processing of personal data by using online services and products. A FIPP explicitly affording individuals the right to veto processing is therefore deemed by established doctrine as unnecessary. The closest the FIPPs come is the Choice and Consent principle which instructs companies to present individuals with choices regarding how their personal data is processed

[36] The question whether personal data can be property has been debated in the academic literature. For some key articles, see Vera Bergelson, It's Personal But Is It Mine? Toward Property Rights in Personal Information, 37 U. of Cal., Davis 379 (2003); Richard S. Murphy, Property Rights in Personal Information: An Economic Defence of Privacy, 84 Geo. L. J. 2381 (1995-1996); Paul M. Schwartz, Property, Privacy, and Personal Data 117(7) Harvard L. Rev. 2056 (2004); Patricia Mell, Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness, 11(1) Berkeley Tech. L. J. 1 (1996); Rochelle Cooper Dreyfuss, Information Products: A Challenge to Intellectual Property Theory 20 N.Y.U. J. Int'l. L. & Pol. 897 (1987-1988); Jessica Litman, Information Privacy/Information Property, 52 Stan L Rev 1283 (2000); Mark A. Lemley, Private Property, 52 Stan L Rev 1545 (2000); Pamela Samuelson, Privacy as Intellectual Property?, 52 Stan. L. Rev. 1125 (2000).

[37] Charles Fried, Contract as Promise: A Theory of Contractual Obligation (2nd ed., Oxford University Press 2015).

– not if it is processed – which may include some rights over secondary uses. FTC guidance delves into the differences between opt-in and opt-out regimes, and the problems that arise in relation to the use of default settings.[38] However, this conceptualization of choice and consent is no longer an accurate reflection of the dilemmas facing the consumer in relation to online commercial surveillance.

The FTC's Choice and Consent principle fails to reflect this reality. The principle also does not reflect the reality mentioned earlier in this report that consumers increasingly have no choice to opt out of using these services, which makes free consent illusory.[39] As is well-known from choice architecture, consent can only be used when there is an actual choice.[40]

The FTC's Choice and Consent principle does not take into account the complexities of what constitutes consent or what the GDPR refers to as 'informed consent.' The difficulties of establishing what constitutes consent – for example the use of tick boxes – is thoroughly reflected in its detailed definition in the GDPR. Article 4(11) GDPR defines consent as, 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.' Conditions for consent is further set out in Article 7 GDPR.

[38] Woodrow Hartzog, Privacy Blueprint: The Battle to Control the Design of New Technologies (Harvard University Press 2018).
[39] ibid.
[40] Cass R. Sunstein, The Ethics of Nudging, 32 Yale J. on Regulation 413 (2015).

It should also be noted that the GDPR does not afford individuals an absolute right to approve of processing of their personal data through consent. Instead, consent is only one of several bases for legal processing set out in Article 6 GDPR, and it is up to the commercial entity to identify which basis is appropriate. There is therefore not the assumption in the GDPR (which is in the FTC's framework) that simply by accepting to use a service or product offered online, that consumers have also consented to have their personal data processed as part of that transaction.

The GDPR also separates the processing of personal data necessary for the performance of a contract and other processing.[41] As such, the GDPR drives a wedge down the middle of the 'personal data in exchange for free services' model. The problem with the 'personal data in exchange for free services' model are numerous. As the default model for social media platforms, it suggests that individuals trade their personal data for the use of 'free' services, meaning they will not pay a subscription fee or similar charge. However, it is not established in jurisprudence that this part of the bargain forms part of a contractual relationship for a host of reasons, not least that the 'consideration' (i.e., payment) individuals pay is too uncertain to be established by a court.

The GDPR reflects this reality by not making consent part of any of its data processing principles. That does not preclude consent from being used – indeed, several provisions in the GDPR allows for the use of

[41] Article 6(1)(b) GDPR.

consent[42] – but that when consent is used, it must be used in line with the data processing principles and the conditions set out in Article 7 GDPR. So while the GDPR in Recital 7 GDPR states that, 'Natural persons should have control of their personal data,' this does not translate into a right to approve or veto processing. Indeed, in adopting the GDPR, EU legislators introduced the accountability principle in Article 5(2) GDPR,[43] thereby emphasizing that the responsibility for these choices should not rest with the consumer, but with the commercial personal data processing entity.

Introducing a mandatory right to consent to the commercial processing of consumer/personal data would be a radical paradigm shift for the FTC. It would recognize consumers as having a default a priori right to their personal data in the context of the marketplace. This conceptualization would depend on the clear identification of consumer/personal data, which is often difficult to do, especially as data is routinely intermingled with the data 'belonging' to other individuals. It would also require companies to inform consumers and demand that consumers make decisions regarding their customer/personal data before it is being processed, even when the data is not directly provided to the company by the consumer in question.

This is near impossible to achieve as only a fraction of the consumer/personal data that is being harvested, processed, and monetized from routinized commercial surveillance is provided

[42] Article 6(1)(a) GDPR for the lawful basis of processing, Article 9(2) GDPR in relation to the processing of special category data, and in relation to some of the user rights in Chapter III GDPR.
[43] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281.

knowingly and directly to a company by the consumer.[44] Consumers are rarely cogent of the hordes of data they constantly feed into the surveillance ecosystem such as metadata, geolocation data, ambient data, and sensory data. Consumers can only make decisions regarding consent over the uses of such data if they are aware that it exists. Companies also generate data to fill in incomplete datasets and for profiling purposes. Such data would also need to be covered by the requirement of consent. The number of consent requests this would entail would be overwhelming and most likely produce consent fatigue and consumer apathy.

Alternatively, consent could be limited to a narrow category of PII. However, in that case, consumers would need to be informed of the limitations of their consent. It is unclear what a narrow category of PII would achieve in practical terms. One way to this could be conceptualized is to limit the scope of consent to only pertain to issues of privacy, but then these would have to be defined. Even so, making decisions regarding information that should be confidential or private is likely to fail as New York University law professor Helen Nissenbaum has argued that privacy is contextual, thus it is the relationship between the parties which determine whether the information should be shared.[45] Still, even a narrowing of scope of individuals' consent over consumer/personal data to data of a private nature would be hard to

[44] See for example the practices of Cambridge Analytica.
[45] Helen Nissenbaum, Privacy in Context: Technology, Policy and the Integrity of Social Life (Stanford Law Books, Stanford University Press 2010).

enforce as once data has been disseminated online it is impossible to recall.

Given the ascent of ubiquitous online commercial surveillance – intensifying at dizzying speed – the notion that individuals will have the cognitive capacity or realistic opportunity to navigate different market products and services for the best match between their personal privacy preferences has become untenable. Routinized commercial surveillance has reached such a magnitude that it is unrealistic that the adoption of a few specific rules will be able to place control over online privacy into the hands of American consumers.

Overall, we recommend that mandatory consent is used in instances where consumers directly provide consumer/personal data to the Internet service provider, online platform, or other provider of services and goods. When consent is used, it must follow similar rules to those set out in Article 7 GDPR to ensure that it is informed and representing the true intention of the consumer. Consent should not be used in situations where the consumer cannot reasonably consent, such as to profiling based on consumer/personal data which has been gathered without the consumer's knowledge. However, the consumer should be alerted to such profiling, and at that point be allowed the choice whether to allow profiling to continue, having received an appropriate explanation of the likely consequences of granting or withholding consent. If consent is denied, the consumer/personal data must be deleted.[46]

[46] This recommendation is in line with the FTC's own recommendation. See FTC (supra note 22), 36-37.

In cases where consent is not used, companies should explain the reasons to consumers. These may include that the data is intermingled with the data of other persons and therefore needs to be kept confidential, trade secrecy requirements, or consent would require more data to be harvested for verification purposes. In cases where individuals cannot be identified or contacted, as in the case of pseudonymous data, the information should be made readily available in generic form in written or verbal notices, as appropriate.

More details regarding our recommendations concerning consumer consent are set out in the appended Q&A document on 'Collection, Use, Retention and Transfer of Consumer Data' and 'Consumer Consent' in response to the FTC's call for responses to Commission File No. R111004.

CONCLUSION AND RECOMMENDATIONS

Routinized commercial surveillance has become ubiquitous, which means that the FTC should adopt new trade regulation rules reflecting this new reality. The FTC is right to consider promulgating new trade regulation rules concerning the use of consumer data to protect consumers and foster trust in the digital economy. It is also right of the FTC to recognize that this responsibility falls under its remit under the FTC Act.

While numerous legislative proposals have been made through the years addressing these issues, none have been passed by US

Congress. While this may change in the near future, it is unlikely that a sole federal statute will have the flexibility and scope to address all of these issues. There are, however, concerted efforts to pass federal privacy legislation, and any rules promulgated must be situated within the evolving statutory context.[47]

Our key recommendations in relation to data processing principles and consumer consent are:

1) Mandatory Data Processing Principles:
    - The FTC should adopt new trade regulation rules which include a mandatory obligation placed on companies to adhere to the transparency, data minimization, purpose limitation, and duration limitation principles in relation to all processing of consumer data.
2) Consumer Consent
    - The FTC should adopt new trade regulation rules governing the use of consumer consent by companies online.
    - Consent should be mandatory in some instances, and whenever used, it should conform to standards similar to those in EU law, including the right to withdrawal consent and the stipulations that consent must be informed.
    - Consent should not be used in situations where the consumer cannot reasonably consent, such as to profiling based on personal data harvested without the consumer's knowledge or understanding.

[47] American Data Privacy and Protection Act, H.R. 8152, 117th Congress (2021-2022).

- Receiving access to goods and services should not be contingent on consent to the processing of personal data unless strictly necessary for the performance of contract or the delivery of those goods or services.

3) Definition of Personal Data
    - The FTC should adopt a definition of personal data that clarifies which data is covered by the data processing principles and consumer consent
    - The definition of personal data should be wider than the definition of 'private' data or 'sensitive' data
    - The definition of personal data should be technologically neutral

Going forward, there are several things the FTC can learn from the EU's GDPR. While taking these lessons on board, it is worth noting that the GDPR essentially demands total surveillance of all personal data. This is a notion that would be anathema to many Americans. The question, however, is not whether commercial surveillance will occur, but whether that surveillance will be regulated by the FTC.

The GDPR data processing principles are fundamental and non-negotiable. The right to data protection in the GDPR is anchored as a constitutional fundamental right in the EU under Article 8 of the Charter of Fundamental Rights of the European Union.[48] Making the European data processing principles mandatory in new trade regulation rules will

[48] 2000/C 364/01. See also Article 16 of The Treaty of the Functioning of the European Union (OJ C 326).

mean that these principles can no longer be deployed as quasi-contractual clauses or competitive advantages. This is likely to affect some companies' USP and intermediary businesses providing privacy-enhancing technologies (PETs) directly to consumers. Instituting new trade regulation rules will undoubtedly add compliance cost to business, particularly in a transition phase. However, this is not novel in the context of consumer protection as business has always had to adapt to new regulatory rules. This is therefore a cost the tech industry should the expected to carry.

Any new trade regulation rules must carefully manage consumer expectations. It is particularly important to recognize that the FTC cannot be a quasi-court for consumers seeking remedies for breaches of the new trade regulation rules. We support the recommendations made by other organizations for affording FTC bolstered enforcement powers.[49] Our point is therefore that it should be for the FTC – not the individual consumer – to be responsible for enforcement. It is also important to keep in perspective that while new trade regulation rules may give consumers more control over the use of their consumer data, they cannot be held responsible for the way it is treated by the tech industry.

It is the tech industry that must be held accountable for its treatment of consumer data. The FTC has a responsibility to ensure that this happens, and new trade regulation rules are crucial to that endeavor.

[49] E.g., Epic.org., What the FTC Could Be Doing (But Isn't) To Protect Privacy, June 2021.

SELECTED BIBILIOGRAPHY

Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Alexandra Korolova, Alan Mislove, Aaron Rieke, Discrimination through optimisation: How Facebook's ad delivery can lead to skewed outcomes, arXiv:1904.0209505, Proceedings of the ACM on Human-Computer Interaction 2019

Kenneth A. Bamberger and Deirdre K. Mulligan, Privacy on the Ground: Driving Corporate Behaviour in the United States and Europe (The MIT Press 2015)

David L. Baumer, Julia B. Earp, J.C. Pointdexter, Internet privacy law: a comparison between the United States and the European Union, 23(5) Computers & Security 400, 400-412 (2004)

Lyra Bennett Moses, Agents of Change: How the Law 'Copes' With Technological Change, 20(4) Griffith L. Rev. 763, 788 (2011)

Vera Bergelson, It's Personal But Is It Mine? Toward Property Rights in Personal Information, 37 U. of Cal., Davis 379 (2003)

Rochelle Cooper Dreyfuss, Information Products: A Challenge to Intellectual Property Theory 20 N.Y.U. J. Int'l. L. & Pol. 897 (1987-1988)

Epic.org., What the FTC Could Be Doing (But Isn't) To Protect Privacy, June 2021

Richard A. Epstein, Law and Economics: Its Glorious Past and Cloudy Future, 64 U. of Chicago L. Rev. 1167 (1997)

Federal Trade Commission, Fair Information Practices Principles: A Practice Statement (1998)

Federal Trade Commission, Privacy Online: A Report to Congress (June 1998)

Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress (2000)

Charles Fried, Contract as Promise: A Theory of Contractual Obligation (2nd ed., Oxford University Press 2015)

Woodrow Hartzog, Privacy Blueprint: The Battle to Control the Design of New Technologies (Harvard University Press 2018

Chris Jay Hoofnagle, Federal Trade Commission: Privacy Law and Policy (Cambridge University Press 2016)

Mark A. Lemley, Private Property, 52 Stan L Rev 1545 (2000)

Meg Leta Jones, The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood, 47 Soc. Stud. Sci. 216 (2017)

Meg Leta Jones, Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw, 2 J. L. Tech. & Pol'y 101, 103 (2018)

Jessica Litman, Information Privacy/Information Property, 52 Stan L Rev 1283 (2000)

Patricia Mell, Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness, 11(1) Berkeley Tech. L. J. 1 (1996)

Arthur R. Miller, The Assault on Privacy: Computers, Data Banks, and Dossiers (The University Press 1970)

Richard S. Murphy, Property Rights in Personal Information: An Economic Defence of Privacy, 84 Geo. L. J. 2381 (1995-1996)

Helen Nissenbaum, Privacy in Context: Technology, Policy and the Integrity of Social Life (Stanford Law Books, Stanford University Press 2010)

Richard A. Posner, The Economics of Justice (Harvard University Press 1983)

Richard A. Posner, Gary Becker's Contribution to Law and Economics, 22(2) The J. of L. Studies 211 (1993)

William L. Prosser, Privacy, 48 Calf. L. Rev. 383, 383 (1960)

Privacy Protection Study Commission ('PPSC'), Personal Privacy in an Information Society (July 1977)

Neil Richards, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (Oxford University Press 2015)

Pamela Samuelson, Privacy as Intellectual Property?, 52 Stan. L. Rev. 1125 (2000)

Paul M. Schwartz, Property, Privacy, and Personal Data 117(7) Harvard L. Rev. 2056 (2004)

Steven Shavell, Foundations of Economic Analysis of Law (The Belknap Press of Harvard University Press 2004)

Daniel J. Solove, Conceptualizing Privacy, 90 Cal. L. Rev. 1087 (2002)

Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Columbia L.J. 583, 583-676 (2014)

Cass R. Sunstein, The Ethics of Nudging, 32 Yale J. on Regulation 413 (2015)

U.S. Department of Health, Education, and Welfare ('HEW'), Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems (July 1973)

Samuel D. Warren, Louis Brandeis, The Right to Privacy, 4(5) Harvard L. Rev. 193, 193-220 (1890)

Alan F. Westin, Privacy and Freedom (Atheneum 1970)

MINDEROO

CENTRE FOR TECHNOLOGY & DEMOCRACY

Alison Richard Building
7 West Road, Cambridge
CB3 9DT

www.mctd.ac.uk

minderoo@crassh.cam.ac.uk

UNIVERSITY OF CAMBRIDGE