A Relational Turn for Data Protection?

*Neil Richards and Woodrow Hartzog**

If there's one thing everyone in the data protection debate can agree on, it's that it's all about the data. All over the world, data protection regimes fixate on when data can be collected, how it is being processed, when it can be accessed or should be deleted, and whether it is personal, sensitive, or deidentified. This is true even for approaches that seem quite different at first glance, such as the U.S. and EU.[1]

But what if our shared focus on the data is too narrow? Data protection as a concept is a relatively new response to a specific technology: the database. In the decades following the Second World War, societies began to realize that data could be aggregated, made searchable, and stored in a pristine state for a remarkably low cost. Lawmakers needed a plan to make sure data could be collected and stored in these databases in a safe and sustainable way. The Fair Information Practices Principle (FIPs), developed with contributions from Americans and Europeans, laid the blueprint for privacy on both sides of the Atlantic.[2] These principles focus on procedural rights like transparency, consent, safeguards, purpose limitations, and data minimization, in service of informational self-determination and a sustainable environment for data processing. Because they emphasize choice and individual autonomy, FIP-based regimes tend to lack substantive prohibitions on particular kinds of data practices. The concept of data protection has been wildly successful in terms of adoption by government and industry. But has it been effective? The jury is still out.

The strongest implementation of the FIPs to date is the GDPR, which has been lauded for its robust and holistic approach. But the GDPR has also failed to reckon with the sheer power of the modern data industrial complex. These companies risk more than just our dignitary interests in our personal data – they control what we see, what we click, and in many cases what we believe. Data is dangerous in the hands of these

* Neil Richards, Koch Distinguished Professor in Law and Director, Cordell Institute, Washington University in St. Louis. Woodrow Hartzog, Professor of Law and Computer Science, Northeastern University.

1 Woodrow Hartzog and Neil Richards, 'Privacy's Constitutional Moment and the Limits of Data Protection' (2020) 61 B C L Rev 1687, 1690-92; James Q Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 Yale L J; Paul Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 NYU L Rev 771; Paul Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy' (2017) 106 Geo L J 115; Paul Schwartz, 'The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures' (2013) 125 Harv L Rev 1966; See William McGeveran, 'Friending the Privacy Regulators' (2016) 58 Ariz L Rev 960 noting some surprising similarities between U.S. and EU approaches; Anupam Chander, Margo Kaminski and William McGeveran, 'Catalyzing Privacy Law' (forthcoming 2021) Minn L Rev.

2 Woodrow Hartzog, 'The Inadequate, Invaluable Fair Information Practices' (2017) 76 Md L Rev 952; Colin J Bennett and Charles D Raab, 'The Governance of Privacy: Policy Instruments in Global Perspective' (2006) 12; Graham Greenleaf, 'Asian Data Privacy Laws: Trade and Human Rights Perspectives' (2014) 6–7; Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press, 2007); Robert Gellman, 'Fair Information Practices: A Basic History' (2016) (unpublished manuscript), <http://bobgellman.com/rg-docs/rg-FIPshistory.pdf>; Chris Hoofnagle, 'The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS)' (2014) (unpublished manuscript) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466418>.

companies not just because it is personal to us, but because in their hands it becomes power that can be wielded to control people and institutions.[3] It exposes us in ways that risk more than just identification or denial of control. Data protection regimes were not designed to confront this kind of adversary.[4] Originating in the 1970s, when home computing and mobile phones were still science fiction in the mode of *Star Trek*, the FIPs were a managerial approach for an analog age. Their approach never questioned that data processing might not always be a worthy endeavor, or that what seemed like large amounts of data in the 1970s might seem quaint a half-century later. Most importantly, the FIPs approach never considered that future consumers and citizens might create so much data and have so many commercial and government accounts that informational self-determination could become impossible. Today, unfortunately, we are living in that never-considered future.

There is, however, a different way to approach data privacy. It has less to do with the data itself and more to do with people and their relationships. Specifically, it looks at how the people who expose themselves and the people that are inviting that disclosure relate to each other. It is concerned with what powerful parties owe to vulnerable parties not just with their personal information, but with the things they see, the things they can click, the decisions that are made about them. It's less about the nature of data and more about the nature of power. And it can make data protection work better. We call this *the relational turn in privacy law*. The folly of our modern privacy predicament is our failure to anticipate the sheer power that results from the scale and size of these large tech companies. We had our eyes trained so much on the data that we lost sight of the power that comes from inequality and inequity in relationships, even when data is fairly processed. But it wasn't always this way.

Long before databases or even film cameras, privacy law was primarily about relationships. American understandings of privacy are traditionally dated to Warren and Brandeis' influential 1890 law review article 'The Right to Privacy,' which called for a cause of action against the press for spreading true but private facts.[5] The authors rested their argument on a large and sometimes ancient body of law protecting information in the context of relationships, including evidentiary privileges, confidential relations, blackmail law, and government records.[6] But unlike studio photographers, married couples, pen-pals, and trustees, the new, aggressive press of the Gilded Age didn't have a relationship with the subjects of its reportage. Warren and Brandeis thus conceived of 'the right to privacy' as tort-based rather than relationship-based, applying weakly to all the world rather than strongly in the context of existing relationships.[7] It focused on

3 Hartzog and Richards (n 1); Julie E Cohen, 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries L 1; Lisa M Austin, 'Enough About Me: Why Privacy is About Power, Not Consent (or Harm), A World Without Privacy? What Can/Should Law Do' (Cambridge University Press, 2014); Daniel J Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2000) 53 Stan L Rev 1393; Carissa Véliz, *Privacy is Power: Why and How You Should Take Back Control of Your Data* (Transworld Digital, 2020).

4 See Hartzog and Richards (n 1); Bert-Jaap Koops, 'The Trouble with European Data Proteciton Law' (2014) 4 Int'l Data Privacy L 250.

5 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harv L Rev 193.

6 Neil M Richards and Daniel J Solove, 'Privacy's Other Path: Recovering the Law of Confidentiality' (2007) 96 Geo LJ 123.

7 ibid, 128-45.

the nature of the data and whether it was public or private, which became a focus on whether data uses were 'highly offensive to a reasonable person' in American tort law, and whether the data being processed was 'sensitive' or not in data protection regimes.[8]

Although the database shifted the focus of privacy law away from relationships of trust for quite some time, America seems to be rekindling its appreciation for them, perhaps recognizing the limits of focusing too closely on the nature of the data and too little on the relationships in which that data is used. A scholarly movement taking relationships seriously in privacy law that began over decade ago is increasingly active and visible.[9] Some scholars (including the authors of this paper), have advocated for legal rules that draw upon the law of fiduciaries to impose duties of loyalty, confidentiality, and care on tech companies as a way of curbing harmful self-dealing and reckless behavior from tech companies in their data processing and the design of their products.[10] Lawmakers in the U.S. have also proposed legislation that cements these duties within information relationships of trust.[11]

The clear advantage of a relational approach is that it is acutely sensitive to the power disparities within information relationships. Tech companies control what we see, what we can click on, and what sorts of information they want to extract from their customers. They have incredible resources that help them predict and nudge our behavior and have the financial incentive to keep us ever more exposed. Duties of loy-

8 ibid, 151, 175.

9 Neil Richards and Woodrow Hartzog, 'Taking Trust Seriously in Privacy Law' (2016) 19 Stan Tech L Rev 431; Neil Richards and Woodrow Hartzog, 'A Duty of Loyalty in Privacy Law' (2020) (unpublished manuscript) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217>; Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' (forthcoming 2019) Wash U L Rev <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3370433>; Neil Richards, Woodrow Hartzog, 'Privacy's Trust Gap' (2017) 126 Yale L J 1180, 1183; Neil Richards and Woodrow Hartzog, 'Trusting Big Data Research' (2017) 66 DePaul L Rev 579; Jack M Balkin, 'Information Fiduciaries and the First Amendment' (2016) 49 UC Davis L Rev 1183, 1185; Jack Balkin and Jonathan Zittrain, 'A Grand Bargain to Make Tech Companies Trustworthy' (2016) The Atlantic (2016), <https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/>; Jonathan Zittrain, 'Engineering an Election' (2014) 127 Harv L Rev F 335, 340; Lindsey Barrett, 'Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries' (2019) 42 Seattle U L Rev 1057; Ariel Dobkin, 'Information Fiduciaries in Practice: Data Privacy and User Expectations' (2018) 33 Berkeley Tech LJ 1, 1; Cameron F Kerry, 'Why Protecting Privacy Is a Losing Game Today—and How to Change the Game' Brookings (2018) <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/>; Ian Kerr, 'The Legal Relationship Between Online Service Providers and Users' (2001) 35 Can Bus LJ 419; Daniel Solove, *The Digital Person* (New York University Press, 2006); Richard S Whitt, 'Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era' (2019) 36 Santa Clara Computer & High Tech LJ 75; Kiel Brennan-Marquez, 'Fourth Amendment Fiduciaries' (2015) 84 Fordham L Rev 611, 612; Lauren Scholz, 'Fiduciary Boilerplate' (2018) J Corp L (forthcoming 2020); Ari Waldman, Privacy as Trust (Cambridge University Press, 2018); Ari Ezra Waldman, 'Privacy As Trust: Sharing Personal Information in A Networked World' (2015) 69 U Miami L Rev 559, 560; Ari Ezra Waldman, 'Privacy, Sharing, and Trust: The Facebook Study' (2016) 67 Case W Res L Rev 193; Christopher W Savage, 'Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy' (2019) 22 Stan Tech L Rev 95.

10 See, eg, Jack Balkin, 'The Fiduciary Model of Privacy' (2020) Harv L Rev F 11; Neil Richards and Woodrow Hartzog, 'Taking Trust Seriously in Privacy Law' (2016) 19 Stan Tech L Rev 431; Neil Richards and Woodrow Hartzog, 'A Duty of Loyalty in Privacy Law' (2020) (unpublished manuscript), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217>; Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018); Neil Richards, *Why Privacy Matters* (forthcoming 2021); *but see* Lina M Khan and David E Pozen, 'A Skeptical View of Information Fiduciaries' (2019) 133 Harv L Rev 497, 498.

11 *See* Data Care Act of 2019, S. 2961, 116th Cong. § 2 (2019) ('Duty of Loyalty: An online service provider may not use individual identifying data, or data derived from individual identifying data, in any way that—(A) will benefit the online service provider to the detriment of an end user; and (B) (i) will result in reasonably foreseeable and material physical or financial harm to an end user; or (ii) would be unexpected and highly offensive to a reasonable end user.'), <https://www.congress.gov/bill/116th-congress/senate-bill/2961/text>; Consumer Online Privacy Rights Act, S.2968, 116th Cong. § 101 ('Duty of Loyalty: (a) In General.—A covered entity shall not—(1) engage in a deceptive data practice or a harmful data practice; or (2) process or transfer covered data in a manner that violates any provision of this Act.'), <https://www.congress.gov/bill/116th-congress/senate-bill/2968/text#toc-idd95044fbea1d498f888e130c44e92067>; New York Privacy Act, S. 5642 (2019), <https://www.nysenate.gov/legislation/bills/2019/s5642> ('Every legal entity, or any affiliate of such entity, and every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances.').

alty protect against self-dealing and duties of care protect against dangerous behavior. The greater the power imbalance and the more people are made vulnerable through exposure, the stricter the duty to which the trusted party is held.[12]

Data protection regimes, by contrast target, imbalances of power within relationships more indirectly by looking to the nature of the data. Rules under the data protection model are largely procedural ones, with a few important exceptions. These provisions are combined with data subject rights against all who process their data, and structural proportions, under the idea fair processing is, in and of itself, a way to mitigate power. But these frameworks are not primarily intended to restrict processing, rather to ensure that processing happens in a legitimate manner.[13] Thus, while relational duties explicitly prioritize the best interests of vulnerable parties, data protection regimes ostensibly pre-code the best interests of data subjects into rules and rights built around the fair information practices. But data privacy should be about more than just the FIPs and informational self-determination.[14] Properly understood, data privacy is about civil rights, free expression, freedom from harassment, collective autonomy interests, and how personal information is leveraged to erode our attention spans, our mental well-being, and our public institutions. The GDPR, CCPA, and other data protection regimes around the world fail to undertake a holistic inquiry that is sufficiently sensitive to such values except in the case of 'legitimate interest' processing.

Data protection frameworks are not agnostic to the status and power of actors, of course. Much hinges on whether people are processors, controllers, or data subjects. But these frameworks typically do not account for the power imbalances between these parties. They essentially treat all relationships between data subjects and controllers the same. Put another way, data protection law flattens the power dynamics of specific relationships, treating your relationship with Google the same the one you have with your grocer. And while Google and your grocer might collect some similar kinds of information in the abstract – your shopping habits and credit card information, for example – you are significantly more vulnerable to Google or any tech platform than you are to your grocer. By controlling your mediated environments in ways that expose you, these companies are able to leverage information they have about you, your network, and people it thinks are similar to you to choose what ads you see, whose posts you see, how you are able to interact with them, and what other people see about you. The relational turn in data privacy rachets up the obligations based in a way that is proportional to this exposure.

We think a relational turn for data protection would be superior to the current model, even of the GDPR, which is still FIPs-based in its bones. A relational turn would provide a path towards more substantive rules that would limit how peoples' data could

12 Balkin, (n 10) 13-14.

13 Eg, Bart van der Sloot, 'The General Data Protection Regulation in Plain Language' (2020) 28-29.

14 Woodrow Hartzog, 'The Inadequate, Invaluable Fair Information Practices' 76 Md L Rev 952 (2017); Hartzog and Richards (n 1).

be used against them. It would focus on the real problem that privacy and data protection law should tackle – the power consequences of information relationships, making legitimacy of processing a question of fundamental fairness rather than data hygiene. Substantive data rules would demand more than that data serve a 'legitimate interest' of the data processor.[15] They would focus on the power consequences of processing on the data subject, whether we apply some version of the classic fiduciary duties of care, confidentiality, and loyalty, or the trust-promoting duties of honesty, protection, discretion, and loyalty that we have called for in other work.[16]

Perhaps equally important, duties of loyalty and care would allow data protection regimes to finally jettison the concept of consent, which it has long been skeptical of. Instead of obsessing over whether the consent people gave was a truly meaningful, informed, and revocable choice, relational duties allow for a decoupling of choice and consent. People would be protected no matter what they choose.[17]

Notably, the European Commission might have just taken the first major step towards a relational turn in E.U. data protection law. On Nov. 25, 2020, the Commission issued a proposal for a regulation on European data governance (Data Governance Act).[18] This proposal includes a remarkable number of bold data privacy interventions designed to increase trust in data intermediaries, including the idea that 'Data sharing providers that intermediate the exchange of data between individuals as data holders and legal persons should, in addition, bear fiduciary duty towards the individuals, to ensure that they act in the best interest of the data holders.'[19] We have long argued for a similarly articulated duty for those entrusted with our information and our online experiences. We think this duty should be the foundation of modern data privacy frameworks and should be applied in a much broader way to encompass all information relationships with significant power disparities.

Much work remains to be done in fleshing out some of the practical the details of the relational turn.[20] Neither Rome nor the FIPs were built in a day, and for all of its flaws, the FIPs model does have the advantage of a half-century's head start. But we worry that if we continue to head down the path of focusing solely on data in service of informational self-determination, it will actually have the effect of continuing to disempower human beings rather than helping them. Ultimately we face a question of what we want the law to do here, and we believe strongly that the informational self-deter-

15 Cf GDPR Art 6.

16 Eg, Neil Richards and Woodrow Hartzog, 'Taking Trust Seriously in Privacy Law' (2016) 19 Stan Tech L Rev 431; Neil Richards and Woodrow Hartzog, 'A Duty of Loyalty in Privacy Law' (2020) (unpublished manuscript) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217>.

17 For an extended critique of consent-based models for data processing, see Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' (forthcoming 2019) Wash U L Rev <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3370433>.

18 European Commission, Proposal for a Regulation on European data governance (Data Governance Act), <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act> (2020).

19 ibid

20 Neil Richards and Woodrow Hartzog, 'A Duty of Loyalty in Privacy Law' (2020) (unpublished manuscript) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217>; Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' (forthcoming 2019) Wash U L Rev <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3370433>.

mination model has been a failure in practice and promises more failure as it confronts the new problems on the horizon: ever-increasing volumes of processing, algorithmic decisionmaking, artificial intelligence, and augmented reality. It's time to try something different. Lawmakers and judges should focus on power and vulnerability and place substantive limitations on the ability of the powerful to manipulate us against our interests. After all, the goal of data protection law should be to promote trust in the digital environment, rather than stoke fear, anxiety, and a sense of being overwhelmed by its complexity. Building trust requires us to focus directly on power imbalances in relationships rather than indirectly through data rules. It's time for data protection's relational turn.