


2020

The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows: Testimony of Professor Neil Richards before the United States Senate

Neil M. Richards

Washington University in St. Louis School of Law, nrichards@wustl.edu

Follow this and additional works at: https://openscholarship.wustl.edu/law_scholarship

 Part of the [European Law Commons](#), [International Law Commons](#), [Legal Studies Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Repository Citation

Richards, Neil M., "The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows: Testimony of Professor Neil Richards before the United States Senate" (2020). *Scholarship@WashULaw*. 527.

https://openscholarship.wustl.edu/law_scholarship/527

This Response or Comment is brought to you for free and open access by the Law School at Washington University Open Scholarship. It has been accepted for inclusion in Scholarship@WashULaw by an authorized administrator of Washington University Open Scholarship. For more information, please contact digital@wumail.wustl.edu.

Prepared Testimony and Statement for the Record

Of

Prof. Neil M. Richards

Koch Distinguished Professor in Law

Director, Cordell Institute for Policy in Medicine & Law

Washington University in St. Louis

Hearing on

**“The Invalidation of the EU-US Privacy Shield and the Future of
Transatlantic Data Flows”**

Before the

Committee on Commerce, Science, & Transportation United States Senate

December 9, 2020

Chairman Wicker, Ranking Member Cantwell, and other distinguished Members of this Committee, thank you for the opportunity to testify at this important hearing examining the future of trans-Atlantic data flows and of American privacy law in light of the European Court of Justice’s invalidation of the Privacy Shield arrangement in the *Schrems 2* case which.¹ My name is Neil Richards, and I am the Koch Distinguished Professor in Law at Washington University in St. Louis, where I also co-Direct the Cordell Institute for Policy in Medicine and Law. I am here as an expert in privacy law, which I have studied, taught, written about, and practiced for the past two decades. I was also asked by the Data Protection Commissioner of Ireland to serve as one of her independent experts in U.S. law in *Schrems 2*, alongside Mr. Andrew Serwin, a distinguished privacy lawyer now with the firm of DLA Piper. The opinions I offer today are my own. They are not necessarily those of either the Irish Data Protection Commissioner or Washington University in St. Louis.

As someone who has followed technology and privacy policy closely since the 1990s, I am deeply encouraged that Congress – and particularly this Committee under Senator Wicker’s and Senator Cantwell’s leadership – is taking seriously the urgent need for comprehensive, reasonable, but consumer protective information privacy legislation. This is something that in my opinion is long overdue – Congress came close to passing such a law in 1974, but failed to reach an agreement on

¹ C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., <http://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=req&pageIndex=1&dir=&occ=rst&part=1&text=&doclang=EN&cid=10716034>. (hereinafter “*Schrems 2*”).

private sector data because of concerns about its effect on industry.² As we know all too well, this is a pattern that has repeated itself all too often over the past fifty years. It is my fervent hope that this time will be different, and that Congress will not just pass a comprehensive privacy bill, but one that gets it right, that provides clear but substantive rules for companies, and which provides adequate protections and effective remedies for consumers. A law that meets these features will not just protect consumers – it will be good for business as well, by helping enable transatlantic data flows and building the consumer trust that is essential for long-term sustainable economic prosperity for all.

In awareness of the limited time I have for these opening remarks, I would like to offer three observations. First, I will explain what I understand the judgment in *Schrems 2* to require, with particular emphasis on factors within the jurisdiction of this Committee. Second, I will illustrate some ways in which this Committee’s work can solve some of the challenges for data flows and privacy law that the *Schrems 2* judgment raises or illustrates. Third, I will argue that this Committee should pass a strong privacy law that builds the consumer trust that is so essential to sustainable and profitable commerce.

² E.g., SARAH E. IGO, *THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICAN* 257-61 (2018); LAWRENCE CAPPELLO, *NONE OF YOUR DAMN BUSINESS: PRIVACY IN THE UNITED STATES FROM THE GILDED AGE TO THE DIGITAL AGE* 200-03 (2019).

I. The *Schrems 2* Case

Privacy is a human right recognized around the world and here in the United States. Protections for privacy run throughout our Constitution, and the “reasonable expectation of privacy” test is at the core of our Fourth Amendment protections against unreasonable searches and seizures.³ As the Supreme Court recognized in the *Carpenter* decision two years ago, these constitutional privacy protections extend to significant categories of human information that are held on our behalf by private companies.⁴ In 1974, when it passed the Privacy Act, Congress recognized that “privacy is a personal and fundamental right.”⁵ Nevertheless, to date, both Congress and the state legislatures have insufficiently protected information privacy against private actors, particularly in the digital context.

Under European law, both privacy and data protection are fundamental rights expressly protected by the European Charter of Fundamental Rights and Freedoms.⁶ In the European Union (EU), the government is required to protect fundamental rights (including privacy rights) against both public and private actors. Consequently, privacy and data protection are specifically protected in the EU by its General Data Protection Regulation or “GDPR.”⁷ As relevant to this hearing, the GDPR does two things. First, it regularizes and limits the collection

³ E.g., *Griswold v. Connecticut*, 381 U.S. 479 (1965); *Katz v. United States*, 389 U.S. 347 (1967); *Riley v. California*, 573 U.S. 373 (2014).

⁴ *Carpenter v. United States*, 585 U.S. ____; 138 S. Ct. 2206 (2018).

⁵ Privacy Act of 1974, § 2(a)(4), P.L. 95-579.

⁶ Charter of Fundamental Rights of the European Union: 2010 O.J. (C83) 389. Proclaimed by the Commission, 7 December 2000. Proclamation and text at 2000 O.J. (C364) 1.

⁷ See Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) (providing the new GDPR).

and processing of personal data by private actors, including companies.⁸ Second, it places limitations on the ability of EU personal data to leave the EU, such as when US tech companies use EU data to fulfill search or GPS requests, store it in the cloud, or use it for HR purposes.⁹ In an ideal case, the GDPR allows the personal data of Europeans to flow to a country whose privacy law has been deemed “adequate.”¹⁰ But American privacy law has never been deemed “adequate,” in large part because America lacks a comprehensive, protective privacy law that allows people to enforce their privacy rights against companies as well as the government.¹¹ As a result, the legality of the trans-Atlantic data trade has been based upon a set of mechanisms that are second-best – including the model contracts and international executive agreements like the Safe Harbor and Privacy Shield at issue in the *Schrems* litigation.

The *Schrems* litigation is a creature of the costly distrust produced by inadequate federal privacy laws, protections, and remedies against both government and corporate surveillance. The first *Schrems* decision of 2015 invalidated the Safe Harbor Agreement based upon the revelations about U.S. Surveillance practices by Edward Snowden.¹² This was replaced by the Privacy

⁸ Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union general data protection regulation: what it is and what it means*, 28:1 Info. & Comms. Tech. L. 65 (2019).

⁹ See Paul M. Schwartz & Karl-Niklaus Peifer, *Transatlantic Data Privacy*, 106 GEO. L. J. 115, 130-31 (2017).

¹⁰ GDPR Art. 45.

¹¹ Paul M. Schwartz & Karl-Niklaus Peifer, *Transatlantic Data Privacy*, 106 GEO. L. J. 115, 158-61 (2017).

¹² 3 Case C-362/14, *Schrems v. Data Prot. Comm’r*, 2015 E.C.R. 650,191 (Oct. 6, 2015).

Shield Agreement, the legality of which was a key issue in the *Schrems 2* litigation. This past July, the European Court of Justice ruled in *Schrems 2*, striking down the Privacy Shield and casting doubt on the mechanism of the standard contractual clauses as a means of transfer to the US.¹³ Because the United States has not been deemed to have an “adequate” level of privacy protections, EU Data Protection regulators are now able to suspend transfers of EU personal data to the United States. Indeed, the Irish Data Protection Commissioner has already initiated such proceedings against Facebook, the American company at issue in the *Schrems* litigation.¹⁴

Two dimensions of the *Schrems 2* holding are of paramount importance to Congress as it confronts privacy reform. The first is that any successor to the Privacy Shield would seem to require Congress to enact surveillance reform. The European Courts are particularly concerned that EU citizens whose data is exported to the United States lack meaningful remedies to challenge the legality of the ways that their data may be processed, and the ways in which it may be accessed (particularly in bulk) by the US Intelligence Community.¹⁵ In particular, the European Court of Justice found in *Schrems 2* that the principal defect of the Privacy Shield mechanism was that it failed to offer a binding legal remedy for violations of EU fundamental data protection rights. The Privacy Shield did not

¹³ See *Schrems 2* at pp. 61-62.

¹⁴ See Shane Phelan & Adrian Weckler, *Facebook in legal battle over order from regulator to halt data transfer to United States*, THE IRISH INDEPENDENT, Sept. 12, 2020, <https://www.independent.ie/business/technology/facebook-in-legal-battle-over-order-from-regulator-to-halt-data-transfer-to-united-states-39524581.html>.

¹⁵ *Schrems 2*, ¶¶ 65, 187, 194.

allow EU citizens to sue the US government for violations of their rights, but it did create an “Ombudsperson” mechanism within the US State Department, who could act as a kind of complaints desk and investigator. As the European Court of Justice put it, however, “there is nothing [] to indicate that [the Privacy Shield] ombudsperson has the power to adopt decisions that are binding on those intelligence services and does not mention any legal safeguards that would accompany that political commitment on which data subjects could rely.... Therefore, the ombudsperson mechanism to which the Privacy Shield Decision refers does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.”¹⁶

The second dimension of the *Schrems 2* decision of relevance to Congress – and of particular relevance to this Committee – is that US privacy laws are not yet “adequate,” which is to say that they do not yet offer protections for personal data held by companies that are “essentially equivalent” to those in the EU. This matters because “adequacy” would let the US be treated essentially as a part of Europe for purposes of EU data flow restrictions. If the US were to be deemed to have an “adequate” level of data protection, then “second-best” mechanisms like the model contractual clauses and Privacy Shield arrangements would become unnecessary. While I understand the kinds of surveillance reforms necessitated by the first dimension of the *Schrems 2* judgment to be more appropriately part of the Senate

¹⁶ *Schrems 2* ¶¶ 196-97.

Judiciary Committee's and Senate Intelligence Committee's jurisdictions, the consumer privacy reforms suggested by the second dimension of the judgment are not merely part of this Committee's jurisdiction, but would seem to me to fall squarely within the bipartisan comprehensive consumer privacy reform project that the Committee has already embarked upon. It is to that issue that I will now turn.

II. Surveillance and Consumer Privacy Reform After *Schrems 2*

As Congress considers comprehensive consumer privacy reform, that reform effort will inevitably intersect with the cross-border data transfer issue raised by the *Schrems* litigation and the invalidation of both the Safe Harbor and Privacy Shield arrangements. To solve the problem of trans-Atlantic data transfers and the GDPR, there are essentially three options. First, the United States could do nothing. This would devastate the lucrative and commerce-enhancing trans-Atlantic data trade and result in so-called "data localization," which would require US companies to build expensive data centers in Europe, and process EU citizens' data there at a significant competitive disadvantage to their international competitors. The second option would be for the Executive Branch to negotiate a third, more-protective version of Safe Harbor/Privacy Shield, which would undoubtedly result in uncertainty as an inevitable "*Schrems 3*" challenge rumbled slowly through the Irish and European Courts once again. While it is impossible to perfectly anticipate the results of such a lawsuit, I can say with confidence that without substantial surveillance and consumer privacy reform, the litigation would be likely to end up

being invalidated on similar grounds to the Safe Harbor Agreement struck down in *Schrems 1* and the Privacy Shield Agreement struck down in *Schrems 2*.

But there is a third way. Comprehensive consumer privacy reform from this Committee, coupled with federal surveillance reform could result not just in another second-best international data transfer agreement, but in an adequacy determination by the European Commission. In fact, the *Schrems 2* judgment points the way towards such an outcome. As the European Court of Justice explained in that case, Article 45(1) of the GDPR permits the European Commission to determine that the US could have an “adequate level of protection.” The European Court of Justice explains further that “the term ‘adequate level of protection’ must, as confirmed by recital 104 of [the GDPR], be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the regulation, read in the light of the Charter.”¹⁷ Article 45 of the GDPR explains this requirement in further detail by explaining that adequacy requires an inquiry into

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that

¹⁷ *Schrems 2* ¶ 94 (citing GDPR Art. 45, GDPR Recital 104).

country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.¹⁸

It is a tremendous (and to my mind disappointing) irony that, even though the Privacy Shield was struck down as insufficient, the privacy protections against commercial processing offered to EU citizens whose data was protected by Privacy Shield was substantially greater than that extended to American citizens under US law.

Yet even if the United States does not seek or achieve an adequacy determination from the European Commission, the level of privacy protection given to personal data in the United States is still relevant to the sustainability of both the model contract mechanism for data transfers and any future, hypothetical “Privacy Shield 2.” This is because, as the *Schrems 2* judgment explains, transfers under the second-best option of model contracts or Privacy Shield-type agreements will still require an inquiry into something very much like the adequacy of data

¹⁸ GDPR Art. 45(2).

protection rights available in the United States.¹⁹ The European Court of Justice specified these requirements clearly as being (1) appropriate safeguards, (2) enforceable rights, and (3) effective legal remedies.²⁰ A few additional observations about what these requirements would mean in practice is warranted, because I think they offer not just a guide to compliance with the GDPR, but also a good road map for US privacy reform. As I understand these concepts, “appropriate safeguards” means that personal information will be processed in ways that are lawful, appropriate, accurate, secure, and not in ways that harm, expose, mislead, misinform, or manipulate American consumers.²¹ “Enforceable rights” means that consumers can make claims against companies regarding how their data is collected, used, and disclosed, whether we are talking about rights of access and correction, rights to prevent the sale or transfer of data for purposes unrelated to the reasons the data was collected in the first place, the placement of duties of care, loyalty, and confidentiality on companies, or independent oversight of commercial uses of data by the FTC or a new independent data protection agency. Finally, “effective legal remedies” means that where consumers have legal rights, they can

¹⁹ *Schrems 2* ¶104 (“The assessment required for that purpose in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country. As regards the latter, the factors to be taken into consideration in the context of Article 46 of that regulation correspond to those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.”); GDPR Art. 46(1) (“In the absence of [an adequacy] a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.”).

²⁰ *Schrems 2* ¶103.

²¹ See Woodrow Hartzog & Neil Richards, *Privacy’s Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020) (suggesting a range of safeguards for American privacy law).

actually vindicate those rights in court, which means private rights of action (whether for damages or injunctive relief) that are not bogged down by excessive administrative exhaustion requirements, corporate *mens rea* requirements, broad statutory defenses and safe harbors, or the difficulties of navigating standing doctrine.

This Committee has already generated draft bills that go a good way towards meeting some of these requirements. For example, Senate Bill 2968, The Consumer Online Privacy Rights Act introduced by Sen. Cantwell, would provide a variety of rights similar (and potentially “essentially equivalent”) to those in the GDPR, like rights of access, deletion, and correction, data minimization, data security requirements to avoid harming consumers, and algorithmic impact assessments.²² The bill would also provide a private right of action for consumers injured by unlawful data processing, something that the challenge of *Schrems 2* seems to require.²³ Senate Bill 2961, The Data Care Act introduced by Sen. Schatz, is a bold and farsighted statute that would place duties of care, confidentiality and loyalty on companies that collect personal data as part of interstate commerce, along with an expansion of FTC and state enforcement authority.²⁴ I am also a fan of some of the provisions of Title II of Senate Bill 4626, The Safe Data Act introduced by Chairman Wicker, which has provisions for algorithmic bias detection, data broker

²² S. 2968, 116th Cong. 1st Sess. (Dec. 3, 2019).

²³ See *id.* tit. III.

²⁴ S. 2961, 116th Cong. 1st Sess (Dec. 2, 2019).

registration, filter bubble transparency, and, critically, abusive trade practices stemming from manipulative interface design.²⁵

These three factors – appropriate safeguards, enforceable rights, and effective legal remedies – are helpful guidelines as this Committee goes about its work. They will be important regardless of whether this Committee seeks an adequacy determination from the European Commission to permit American companies to participate in the trans-Atlantic data trade, whether this Committee wants to avoid another *Schrems 1* or *Schrems 2*, whether this Committee wants to give American consumers equivalent protection under American law to that which EU consumers received under the Privacy Shield, or whether this Committee merely wants to pass a meaningful consumer privacy protection bill that protects American consumers and provides clear but meaningful protective guard rails for companies to stay within as part of the digital economy.

With respect to this process going forward, however, let me be clear about three essential features that I believe consumer privacy reform in the United States must recognize. First, the model of “notice and choice” under which the United States has regulated privacy for the past twenty-five years has been an unmitigated disaster. Constructive “notice” through privacy policies and fictitious “choice” through limited opt-outs have created both an illusion of consumer control and enabled largely unrestricted data aggregation.²⁶ Our law has not given consumers

²⁵ S. 4626, 116th Cong. 2d Sess. (Sept. 17, 2020).

²⁶ See, e.g., Neil Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law 19 STAN. TECH. L. REV. 431 (2016); Neil Richards & Woodrow Hartzog, The Pathologies of Digital Consent, 96

control; it has instead left them largely defenseless and able to be tracked, sorted, harmed, discriminated against, marketed to, ideologically polarized, and manipulated by private companies. Any meaningful privacy reform that is “consumer protective” in anything more than name, must place substantive limits on the ability of companies to collect, use, and sell personal data without meaningful constraint.²⁷

Second, as the European Court of Justice recognized, private rights of action are an essential tool for vindicating legal rights. America’s next-generation privacy law should not authorize “gotcha” private claims, or massively aggregated class action suits that risk ruinous liability for technical violations. But it should provide what the European Court of Justice calls both enforceable rights and effective legal remedies, even if such remedies offer in some cases “merely” effective injunctive relief to prevent violations.

Third, and finally, I have concerns about bills that are broadly pre-emptive of state causes of action. State legislatures and state attorneys general have often valiantly protected consumer privacy rights in the digital age in the absence of a general federal privacy law.²⁸ They have invented new and needed legal protections like data breach notification laws, which have spread throughout the country and

WASH. U. L. REV. 1461, 1463 (2019); Woodrow Hartzog & Neil Richards, *Privacy’s Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020).

²⁷ See, e.g., Neil Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law 19 STAN. TECH. L. REV. 431 (2016); Neil Richards & Woodrow Hartzog, The Pathologies of Digital Consent, 96 WASH. U. L. REV. 1461, 1463 (2019); Woodrow Hartzog & Neil Richards, *Privacy’s Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020).

²⁸ See Danielle K. Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2017).

around the world.²⁹ The great American jurist Louis Brandeis famously referred to state regulatory experimentation as our “laboratories of democracy,”³⁰ and in this time of uncertainty and rapid technological change, we should be reluctant to deprive ourselves of this opportunity for regulatory innovation. Moreover, where state private causes of action like negligence or the privacy torts are sometimes the only form of relief available to plaintiffs, I believe that it would be unwise for a federal law to pre-empt state causes of action, at least without providing equivalent federal protections.

²⁹ California passed the first data breach notification law in 2012. See CAL. CIV. CODE §§ 1798.29, .82, .84 (2012). Today, not only do state data breach laws apply across the United States, but federal laws like the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley Act also contain notification requirements, and even the GDPR has incorporated this American legal invention into its comprehensive regulatory scheme. See 16 C.F.R. § 682.3(a); 45 C.F.R. §§ 164.308-.314; 16 C.F.R. §§ 314.3-314.4; ALASKA STAT. § 45.48.010 et seq. (2007); ARIZ. REV. STAT. § 44-7501 (2013); ARK. CODE § 4-110- 101 et seq. (2004); CAL CIV. CODE §§1798.29, .82, .84 (2012); COLO. REV. STAT. § 6-1-716 (2002); CONN. GEN. STAT. § 36a-701b (2011); DEL. CODE Tit. 6, § 12b-101 et Seq. (2011); FLA. STAT. §§501.171, 282.0041, 282.318(2)(I) (2010); GA. CODE §§ 10-1-910, -911, -912 § 46-5-214 (West); HAW. REV. STAT. § 487n-1 et seq.(2008); IDAHO STAT. §§ 28-51-104 To -107 (2008) ; 815 ILL. COMP. STAT. ANN. §§ 530/1 to 530/25 (2008); IND. CODE §§ 4-1-11 et seq., 24-4.9 et seq.(2014); IOWA CODE §§ 715c.1, 715c.2 (2015); KAN. STAT. § 50-7a01 et. seq. (2008); KY. REV. STAT. ANN. §§ 365.732, 61.931 To 61.934 (West); LA. REV. STAT §§ 51:3071 et seq. 40:1300.111 To .116 (West); ME. REV. STAT. tit. 10 § 1347 et seq. (2009); MD. CODE COM. LAW §§ 14-3501 et seq. (2013), MD. STATE GOVT. CODE §§ 10-1301 To -1308 (2007); MASS. GEN. L. § 93h-1 et seq. (2006); MICH. COMP. LAW §§ 445.63,445.72 (2014); MINN. STAT. §§ 325e.61, 325e.64 (2011); MISS. CODE § 75-24-29 (2014); MO. REV. STAT. § 407.1500 (2014); MONT. CODE §§ 2-6-504, 30-14-1701 et seq. (2014); NEB. REV. STAT. §§ 87-801, -802, -803, -804, -805, -806, - 807 (2014); NEV. REV. STAT. §§ 603.A.010 et seq., 242.183 (2013); N.H. REV. STAT. §§359-C:19, -C:20, - C:21 (2009); N.J. STAT. ANN. § 56:8-163 (2012); N.Y. GEN. BUS. L. § 899-Aa, N.Y. STATE TECH. L. 208 (McKinney 2014); N.C. GEN. STAT. §§ 75-61, 75-65 (2012); N.D. CENT. CODE § 51-30-01 et seq (2008).; OHIO REV. CODE §§ 1347.12, 1349.19, 1349.191, 1349.192 (2004); OKLA. STAT. §§ 74-3113.1, 24-161 to -166 (2014); OR. REV. STAT. § 646a.600 to .628 (2011); 73 PA. STAT. §2301 et seq. (2013); R.I. GEN. LAWS § 11-49.2-1 et seq. (West); S.C. CODE § 39-1-90 (West); TENN. CODE § 47-18-2107 (2014); TEX. BUS. & COM. CODE §§ 521.002, 521.053 (2014), TEX. ED. CODE § 37.007(B)(5) (2013); UTAH CODE §§ 13-44-101 et seq. (2010); Vt. Stat. Tit. 9 § 2430, 2435 (2007); Va. Code § 18.2-186.6, § 32.1-127.1:05 (2012); WASH. REV. CODE § 19.255.010, 42.56.590 (2013); W.V. CODE §§ 46a-2a-101 et seq. (West); WIS. STAT. § 134.98 (2009); WYO. STAT. § 40-12-501 et. seq. (2007); D.C. CODE § 28-3851 et seq. (2013); 10 LAWS OF PUERTO RICO § 4051 Et Seq.; V.I. CODE TIT. 14, § 2208.

³⁰ *New State Ice Co. v. Liebmann*, 285 U.S. 262 (1932).

III. Strong Privacy Safeguards Build Consumer Trust

The *Schrems 2* litigation has certainly created problems for American privacy law, but it has also created a pathway towards the resolution of those problems, whether through an adequacy determination, comprehensive privacy and surveillance reform, or both. In the time that I have left, however, I would like to make one final point, which is that as this Committee considers privacy reform it give serious consideration to imposing some kind of duty of loyalty on data processors. In my work with Professor Woodrow Hartzog of Northeastern University, I have argued that the solution to the problems of American privacy lies in building trust. Today we face a crisis of distrust. The Snowden revelations created justifiable distrust when Americans and Europeans across the political spectrum realized the scope of largely unconstrained surveillance by the Intelligence Community. The *Schrems* litigation is a further offshoot of this distrust by European consumers, regulators, and judges. Distrust harms everyone – consumers, businesses, and government. It most certainly is bad for business in our modern data-driven economy.

There is a better way than our status quo of distrust. In a series of articles, Professor Hartzog and I have sought to identify the factors that could get us beyond the dangerous fiction of “notice and choice” privacy regulation, and use privacy law to create value for companies as well as protecting consumers. Our trust theory suggests that companies who seek trust must be discreet, honest, protective, and

loyal.³¹ In a forthcoming article, we give greater detail to a duty of loyalty for privacy law based on the risks of opportunism that arise when people trust others with their personal information and online experiences. Data collectors bound by a duty of loyalty would be obligated to act in the best interests of the people exposing their data and engaging in online experiences, but only to the extent of their exposure. Loyalty would manifest itself primarily as a prohibition on designing digital tools and processing data in a way that conflicts with a trusting parties' best interests. Our basic claim is simple: a duty of loyalty framed in terms of the best interests of digital consumers should become a basic element of U.S. data privacy law. A duty of loyalty would compel loyal acts and also constrain conflicted, self-dealing behavior by companies. It would shift the default legal presumptions surrounding a number of common design and data processing practices, and it would act as an interpretive guide for government actors and data collectors to resolve ambiguities inherent in other privacy rules. A duty of loyalty, in effect, would enliven almost the entire patchwork of U.S. data privacy laws. And it would do it in a way that is consistent with American law and traditions, including its commitments to free expression goals and other civil liberties. A duty of loyalty along the lines we suggest would be a big step for American privacy law, but we think it would be a necessary and important one if our digital transformation is to live up to its great promises of human wellbeing and flourishing. It would also be good for business over the long term. The relationship between privacy and trust

³¹ Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap*, 126 YALE L.J. 1180, 1183 (2017).

has been the subject of a lively and creative academic literature.³² We also note with optimism that the duty of loyalty is a topic of debate on this Committee, and we hope that this Committee will take the duty of loyalty seriously as an opportunity to protect consumers, safeguard responsible, sustainable commerce, and allow the United States to once again become a leader in global privacy norms.³³

Conclusion

Thank you for giving me the opportunity to share my views on the consequences of the *Schrems 2* decision for privacy reform in the United States. In sum, the *Schrems* litigation is a creature of distrust, and while it has created

³² Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty in Privacy Law*, (Sept. 5, 2020) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217; Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, WASH. U. L. REV. (forthcoming 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3370433; Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap*, 126 YALE L.J. 1180, 1183 (2017); Neil Richards & Woodrow Hartzog, *Trusting Big Data Research*, 66 DEPAUL L. REV. 579 (2017); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1185 (2016); Jack Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, THE ATL. (Oct. 3, 2016), <https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/>; Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335, 340 (2014); Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057 (2019); Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 1 (2018); Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS (July 12, 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*, 35 CAN. BUS. L.J. 419 (2001); Daniel Solove, *THE DIGITAL PERSON* (2006); Richard S. Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era*, 36 SANTA CLARA COMPUTER & HIGH TECH. L.J. 75 (2019); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 612 (2015); Lauren Scholz, *Fiduciary Boilerplate*, J. CORP. L. (forthcoming 2020); ARI WALDMAN, *PRIVACY AS TRUST* (2018); Ari Ezra Waldman, *Privacy As Trust: Sharing Personal Information in A Networked World*, 69 U. MIAMI L. REV. 559, 560 (2015); Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, 67 CASE W. RES. L. REV. 193 (2016); Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95 (2019).

³³ See Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, forthcoming 2021, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217.

problems for American law and commerce, it has also created a great opportunity. That opportunity lies before this Committee – the chance to regain American leadership in global privacy and data protection by passing a comprehensive law that provides appropriate safeguards, enforceable rights, and effective legal remedies for consumers. I believe that the way forward can not only safeguard the ability to share personal data across the Atlantic, but it can do so in a way that builds trust between the United States and our European trading partners and between American companies and their American and European customers. I believe that there is a way forward, but it requires us to recognize that strong, clear, trust-building rules are not hostile to business interest, that we need to push past the failed system of “notice and choice,” that we need to preserve effective consumer remedies and state-level regulatory innovation, and seriously consider a duty of loyalty. In that direction, I believe, lies not just consumer protection, but international cooperation and economic prosperity. Thank you.

Biography

Neil Richards is one of the world's leading experts in privacy law, information law, and freedom of expression. He writes, teaches, and lectures about the regulation of the technologies powered by human information that are revolutionizing our society. Professor Richards holds the Koch Distinguished Professorship at Washington University School of Law, where he co-directs the Cordell Institute for Policy in Medicine & Law. He is also an affiliate scholar with the Stanford Center for Internet and Society and the Yale Information Society Project, a Fellow at the Center for Democracy and Technology, and a consultant and expert in privacy cases. Professor Richards serves on the board of the Future of Privacy Forum and is a member of the American Law Institute. Professor Richards graduated in 1997 with graduate degrees in law and history from the University of Virginia, and served as a law clerk to both William H. Rehnquist, Chief Justice of the United States and Paul V. Niemeyer, United States Court of Appeals for the Fourth Circuit.

Professor Richards is the author of *Intellectual Privacy* (Oxford Press 2015). His many scholarly and popular writings on privacy and civil liberties have appeared in wide a variety of media, from the *Harvard Law Review* and the *Yale Law Journal* to *The Guardian*, *WIRED*, and *Slate*. His next book, *Why Privacy Matters*, will be published by Oxford Press in 2021.