

**Before the  
Federal Trade Commission  
Washington, DC**

In the Matter of: )  
)  
Developing the FTC's ) Docket No. FTC-2018-0098  
Approach to Consumer Privacy )  
)  
)

**Comments of Privacy Without Borders**  
at [privacywithoutborders.org](http://privacywithoutborders.org)

via upload files at  
[https://www.regulations.gov/  
comment?D=FTC-2018-0098-0003](https://www.regulations.gov/comment?D=FTC-2018-0098-0003)

Steven Hoffer, CIPP/US/E  
Founder & General Counsel

December 21, 2018

[hoffersteven@gmail.com](mailto:hoffersteven@gmail.com)  
415.500.1878

Privacy Without Borders  
[@privacywithoutborders.org](http://privacywithoutborders.org)  
Department of Law & Policy

**COMMENTS**

I. Introduction

The FTC's initiative to explore consumer privacy reforms in view of policy and enforcement goals has been widely welcomed and applauded. It demonstrated the growing need for greater assessment, legislative action, and cooperation by all Federal government branches. It also recognized that the U.S. ought to cross-reference data protection laws recently updated abroad. The U.S. can ensure best the convergence in norms for the recognition and enforcement of privacy rights of individuals through meaningful rules for a baseline of data protection across all sectors of industry.

The vast majority of Americans seek to share high levels of data protection of their personally identifiable information (PII) that places them first among equals with respect to other citizens abroad residing in advanced democracies. Many of our trading partners abroad already ensure that data protection and privacy rights are comprehensively protected and remain enforceable by individuals directly, with only limited exceptions.

## 2. Legal Frameworks and Reforms

The FTC asks "[w]hat are existing and emerging legal frameworks for privacy protection? What are the benefits and drawbacks of each framework?"

The FTC itself offered part of the answer upon noting that some nations have enacted legislation for comprehensive data privacy protection regimes, while others like the U.S. have relied on sectoral privacy laws. Specifically, the FTC's notice for these comments reflects that "[s]ome jurisdictions have enacted new laws that contain new approaches for addressing privacy risks. The European Union, for example, enacted the General Data Protection Regulation (GDPR) (effective in May 2018), which includes data access, erasure, and portability rights and breach notification requirements."

The FTC also refers to recent comments on key privacy principles collected by NTIA. Some of the comments to the NTIA elaborated on the risks and benefits of the different kinds of frameworks, including comprehensive, sectoral, and hybrid regimes, as well as convergence trends. A transition from notice-and-consent regimes to a risk-based approach under laws enacted by certain U.S. states also has provided some promising advances, but still something more is needed to raise a higher default level of privacy.

Many of the common legal principles of U.S. privacy law truly favor conformity with the law of nations. These common principles also appear to support additional U.S. reforms to close other gaps at least through regulatory convergence, if not full harmonization. Like other common cross-border norms that range from cyber-security to cooperative evidentiary rules, the better rules of consumer privacy across the United States share common principles with data protection norms in the EU, including requirements of notice, consent, purpose limitations, confidentiality, integrity and availability. They also require stronger safeguards for higher risk operations. The FTC should recognize that greater cross-border cooperation and legal convergence could safeguard international data flows, with predictable benefits, from sudden disruption.

New U.S. regulations must advance many common policies in view of public frustration with data breaches in a global economy characterized by growing volumes of

personal data flows, trade in services, ecommerce, data brokers, big data, behavioral advertising, AI, mobility, and cloud computing. These factors also underscore the scale of the cross-border legal and regulatory challenges. They weigh strongly in favor of continuing the momentum by U.S. authorities to stretch toward developing shared global privacy norms that are in balance with other individual rights of Americans.

A newly emerging U.S. framework will either reinforce or obstruct common cross-border privacy rules and data protection norms required for efficient economic integration. For the NTIA, a coalition of privacy scholars<sup>1</sup> aptly observed that:

Creating a larger gap between U.S. and European data privacy law will threaten already at-risk legal regimes for transferring data between those parts of the world.<sup>2</sup> This will raise, not lower costs, for companies doing business around the globe. \*\*\*\* [I]f NTIA decides to treat federal privacy legislation as a floor, this would not only increase harmonization with global standards, it might significantly lower global compliance costs for companies, while also raising protections for U.S. citizens. Any discussion of harmonization must take into account not just state-federal dynamics, but federal-global dynamics as well.

As a corollary, new U.S. statutes or regulatory measures that actually weaken consumer privacy protection via Federal law, or that preempt stronger protections emerging under state laws, could leave Americans with sub-standard data privacy protection for several decades. Absent convergence, all keen observers will foresee a costly and widening rift from a hefty shift in western privacy injuries to American.<sup>3</sup>

The limited extent of administrative law discretion of the FTC also fails to adequately ensure that the FTC may wield the requisite enforcement authority to substantially equalize the levels of data protection domestically with the EU under the prevailing two prongs of Section 5 of the FTC Act, to wit: (a) deceptive practices and (b) unfair practices.<sup>4</sup> The FTC Act and related laws are unduly limiting and too encumbered by stale policies and statements with prior constraints. While the two prongs are necessary, they are not sufficient enabling statutes. When viewed narrowly by courts, the limited ambit of FTC authority solely to address violations of consent decrees merely with specific fixed remedial measures that are insensitive to changing risk parameters

---

<sup>1</sup> See Comments of Privacy Law Scholars for NTIA at 47 - 48 (November 9, 2018).

<sup>2</sup> Id., citing INT'L. TRADE ADMIN., Privacy Shield Overview, <https://www.privacyshield.gov/Program-Overview>. (original)

<sup>3</sup> Id. at 47-48(also noting that dismantling strong state privacy laws via preemption could undermine a key mechanism for transfer of EU data to the U.S., under the Privacy Shield).

<sup>4</sup> 15 U.S.C. § 45(a)(1) (limiting FTC jurisdiction to “unfair or deceptive acts or practices in or affecting commerce”).

misses the mark. This view remains an anachronistic vestige from the back half of the last century. Worse still, without broader powers vested in the FTC, the PII of Americans would become the "lowest hanging fruit" for abusive practices of data brokers and hackers alike.<sup>5</sup> The FTC ought to urge Congress to enact additional statutes to enable the FTC to enforce risk-benchmarked requirements in view of prior consent decrees and binding sanctions. It should especially impose such sanctions on data-intensive enterprises that violate consumer privacy or other data protection rights.

FTC regulatory reforms on PII must start by carefully drafting supplemental enabling legislation or statutory amendments. Within America, privacy scholars have already explained why state laws should only be pre-empted if and when Federal law harmonizes up the standards of protections toward the higher end of range of protection offered under the welter of U.S. state laws. The FTC's current enforcement practice does not sufficiently dissuade big data companies, data brokers, and data miner from passively condoning unauthorized transfers of personal data. They also cavalierly mischaracterize data breaches as merely pesky incidents amounting to something less egregious.<sup>6</sup> The role of the FTC should be a leading one that retains and wields authority to impose a baseline of protection over the conduct of nearly all interstate businesses that process PII.

### 3. The Role of The FTC as the Main American Data Protection Authority

The FTC requires expanded rule-making and enforcement authority calibrated to heightened risks to PII in the current century. A proper expansion will permit the FTC to promulgate more stringent substantive binding rules across unregulated industries, and especially ones where PII and network effects are combined.<sup>7</sup>

An independent data protection agency like the FTC ought to be unequivocally conferred authority in the first instance to enforce rules upon businesses other than some exempt low-risk businesses, like ones described further below.<sup>8</sup> The distinction between legislative rules (that is, substantive legislative rules) and other types of rules is important in administrative law for several reasons. One is that the Administrative Procedures Act (APA) generally requires other agencies to engage in notice- and-comment rulemaking before making legislative rules, but not before making procedural rules, interpretative

---

<sup>5</sup> Imagine, for instance, if only Europeans were eligible to seek the shelter of Do Not Call lists, and Americans by default bore a disproportionate targeting by telemarketers worldwide.

<sup>6</sup> As one point of departure, the FTC should urge adoption of a new law to unify a national norm for a breach notification period that is toward the shorter end of the range of intervals prescribed by the states, in view of the EU three day standard, so that Federal period would preempt any state law that would otherwise extend the notice due dates or broaden exemptions.

<sup>7</sup> See also, Comments of Privacy Law Scholars for NTIA, *infra* at note 1, at 42-43.

<sup>8</sup> See, e.g., Peter P. Swire Elephants and Mice Revisited: Law and Choice of Law on the Internet, 153 U. Pa. L. Rev. 1975 (2005).

rules, or policies.<sup>9</sup> Congress should deliberate the merits of either (a) bringing back the exercise FTC authority under APA norms, or (b) refining alternatives processes to advance the FTC's power via precedential quasi-judicial administrative cases.

New enabling legislation ought to delegate more enforcement authority<sup>10</sup> and introduce provisions that envision *precedential* complaint decision jurisdiction at the FTC.<sup>11</sup> In LabMD v. The Federal Trade Commission, the Eleventh Circuit Court of Appeals ruled against sustaining the FTC's order after indicating, in *dicta* that follows, how the Chevron standard applied to the FTC:

We recognize that the FTC's interpretation of § 45(n) is entitled to Chevron deference, if it is reasonable. See Chevron U.S.A. Inc. v. Nat. Res. Def. Council, 467 U.S. 837, 842–43, 104 S. Ct. 2778, 2781–82 (1984); United States v. Mead Corp., 533 U.S. 218, 226–27, 229, 121 S. Ct. 2164, 2171, 2172 (2001). We also know the Supreme Court has specifically instructed that “Congress intentionally left development of the term ‘unfair’ to the [FTC]” because of “the many and variable unfair practices which prevail in commerce.” Atl. Ref. Co. v. FTC, 381 U.S. 357, 367, 85 S. Ct. 1498, 1505 (1965) (quotation omitted).<sup>12</sup>

In the end, however, it reasoned that LabMD could not be commanded to replace its data-security program to meet an indeterminable standard of reasonableness.

To better ensure that the FTC may dynamically update the standards of reasonableness to address rapid technological changes, particularly in view of prior

---

<sup>9</sup> Since A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495 (1935), the Supreme Court has redefined the measures with which the judicial branch may define the scope of authority delegated by Congress to administrative agencies of the Executive branch. See also, Am. Mining Congress v. Safety & Health Admin., 995 F.2d 1106, 1109 (D.C. Cir. 1993); American Postal Workers Union v. U.S. Postal Service, 707 F.2d 548, 558 (D. C. Cir. 1983) (“A rule can be legislative only if Congress has delegated legislative power to the agency and if the agency intended to use that power in promulgating the rule at issue.”); cf. Joseph v. U.S. Civil Serv. Comm'n, 554 F.2d 1140, 1153 n.24 (D.C. Cir. 1977).

<sup>10</sup> In Chevron USA, Inc. v. Natural Resources Defense Council, 467 U.S. 837 (1984), the Court clarified the rule of deference to reasonable agency interpretations of ambiguous statutory provisions. The Court later held in United States v. Mead Corp., 533 U.S. 218 (2001)(J. Scalia dissenting) that agency interpretations are entitled to Chevron deference only when Congress has delegated power to the agency to make rules with the force of law and the agency's interpretation was rendered in the exercise of that power. The first step of this inquiry, however, is often difficult to apply because the typical rulemaking grant falls short of specifying whether the “rules and regulations” have the force of law, or includes only procedural and interpretative rules.

<sup>11</sup> LabMD v. FTC, No. 16-16270, slip op., (11th Cir. June 6, 2018)(The court held that the FTC's prohibitions contained in the cease and desist orders and injunctions must be specific, otherwise they may be unenforceable).

<sup>12</sup> See *Id.*, at 7.

consent decrees, the FTC should prepare proposed legislative reforms to expressly extend the FTC's interstate jurisdiction over consumer privacy in the public interest both within and beyond the extant two-prong delegation. FTC jurisdiction, for instance, ought to allow exercises of discretion to prevent the transgression of rights under either the FIPP principles or currently prevailing data-security requirements, even if only by reference to consent decrees with specified requirements, versioned specifications, updated codes of conduct, benchmarks, or risk-calibrated safeguards.<sup>13</sup>

A. The FTC's Role Includes Rule-Making to Protect PII

The FTC should be able, to issue a Notice of Proposed Rule Making (NPRM) to promulgate a reasonably acceptable data protection standard and data security baseline. For instance, it should be able to issue a NPRM to explore whether to establish and normalize across domestic interstate commerce a consumer right to opt-out of having personal information sold from one organization to another, as reflected in the California Consumer Privacy Act.

Another preliminary inquiry may be overdue as to the key question: who controls or owns the personal data at issue? This question again underscores that there are two kinds of challenges that the FTC ought to address: (i) how to regulate the secondary uses of a massive volume of PII already presently accumulated by businesses and (ii) how to imposed data minimization duties upon business engaged on-going and future PII collection or processing.

For the first kind of challenge, the FTC should consider that separate data brokers and miners already maintain access to over 3,000 data points on nearly each adult in the U.S. As such, the FTC should issue a further NPRM to ascertain whether these identifiable adults, and similarly identifiable children, can exercise rights of retroactive ownership and control, which include rights of access, correction, and deletion. Deletion and limited retention should be mandated absent periodic reconfirmations of opt-in consent to restrict undue secondary use or transfers.<sup>14</sup> The FTC should use its authority

---

<sup>13</sup> See, e.g., Kamala D. Harris, Attorney General California Dept. of Justice, California Data Breach Report 2012-2015 (2016), at Appx. A - C. viewed at <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>

<sup>14</sup> Executive Office of the White House, Big Data; Seizing Opportunities, Preserving Values, May 2014 ("BIG DATA"). Even in May, 2014, the magnitude of the burgeoning problems that afflict the public via the Advertisement Ecosystem and "Unregulated Data Brokers" were evident:

"To assist marketers, data brokers can provide a profile of a consumer who may interact with a brand or seek services across many different channels, from online web presence to social media to mobile engagement. Data brokers aggregate purchase patterns, activities on a website, mobile, social media, ad network interactions, or direct customer

aggressively to enforce sanctions on businesses that disregard the limited purpose principle, fail to limit retention, or decline requested erasure such PII data without just cause. The FTC ought to be able to suspend further PII processing absent opt-in consent records, impose constructive trust requirements, require divestiture of misused data assets, or apply and enforce fiduciary duties.

For the second kind of challenge, the FTC should investigate how to impose data minimization standards to avoid further excessive collections and future processing of PII. It should codify clear rules to avoid unauthorized access to PII via tracking, mining, transfer, and inferential linking techniques. The health informatics industry has already reached the correct answer: the patient owns his or her data.<sup>15</sup> Moreover, as to sensitive data, the burden must be placed squarely on the controllers and processors to refrain from processing PII, unless they can show specific, expressed, and unambiguous consent by a person who opts-into data sharing process. The advent of more powerful analytics, which can discern quite a bit from even small and disconnected pieces of data, raises the possibility that data gathered and held by third parties can be amalgamated and analyzed in ways that reveal even more information about individuals.<sup>16</sup>

The FTC, absent congressional enactments, must delimit a test, or set of criterion, to ascertain expressly when it is necessary to promote some conflicting interest to supersede the data protection interests of the individual, and where the doctrine of proportionality may dictate that the data protection right of the individual must yield to the conflicting interest.<sup>17</sup> While the principle of proportionality may be helpful, the

---

support, and then further 'enhance' it with information from public records or other commercially available sources. That information is used to develop a profile of a customer, whose activities or engagements can then be monitored to help the marketer pinpoint the message to send and the right moment to send it.

These profiles can be exceptionally detailed, containing upwards of thousands of pieces of data. Some large data firms have profiles on hundreds of millions of consumers. They algorithmically analyze this information to segment customers into precise categories, often with illustrative names that help their business customers identify populations for targeted advertising." *Id.* at 44

<sup>15</sup> See, e.g. Comments of the AMIA to NTIA, November 9, 2018 at 2. ("AMIA believes that patients should always have access to and control over their health data (footnote omitted). This operating principle should not only apply to the health sector, but across all sectors of the U.S. economy. ... *AMIA recommends that consumer access to and control of his or her data be a prerequisite condition and central organizing principle from which other outcomes derive.*"(Emphasis original).

<sup>16</sup> BIG DATA, *infra* at note 14. at 34. Notably, only three data points are needed today to identify most Americans: date of birth, gender, and zip code.

<sup>17</sup> Data protections need not be absolute to be protected more vigorously at a high level. Unlike the E.U., any professed right to be forgotten (RTBF), for instance, could be appropriately limited

proper rules must ordinarily place the onus on the one advocating the conflicting interest further to show predominance of the conflicting interest and that less restrictive alternatives could not similarly promote that objective or achieve that interest.

To this end, the doctrine of proportionality for consumer privacy may be applied, or may be interpreted as a sliding standard of review much like the ones governing free speech under the First Amendment. In other words, data privacy also may be tested via a protean standard that has at least three tests including strict scrutiny, intermediate scrutiny, and the rational-basis scrutiny, similar to ones used in First Amendment cases.<sup>18</sup>

For instance, using proportionality, the FTC may adopt an exemption to the general rule for enforcing stringent data protection in low-risk contexts. For instance, the FTC ought to be able to confer an exemption by rule upon certain small businesses and start-up operators to advance innovation and competition. Those entities entitled to this exemption should be defined as those who are eligible to receive small business treatment and loans under Federal law, provided also that they are neither (i) engaged in the processing of sensitive data, nor (ii) in the primary line of business of processing or brokering large volumes of personal data (hereafter "exempt businesses"). This idea of delineating exemptions also may be reconciled with a baseline of data protection that ensures fundamental rights of data protection for higher risk operations broadly under various levels of scrutiny described herein, irrespective of the size of the processor.<sup>19</sup>

Whether the FTC will find potential abuse in data collection, processing, brokering, AI, or cloud computing, it must exercise more proactive rulemaking authority just to keep pace with the accelerating rate of change. New baseline U.S. standards are needed to anticipate and govern unfettered use of inference-based algorithms that may introduce a likelihood of unduly discriminatory pricing, precipitate risks of restraints of trade, or perpetuate invidious biases that erode equal treatment.

The FTC's policy goals and enforcement practices must not be diluted nor succumb to extreme political swings of the prevailing administration or partisanship in Congress, particularly when the Supreme Court is already empaneled with jurists with the most pro-business views in modern history. At minimum, the FTC should dispense adopting the talking points of coalitions of big business, data miners, and Big Data constituents even as a point of departure for further analysis. Otherwise, doing so would

---

to areas that do not preserve false representations, or otherwise do not unduly subordinate opposing rights that should predominate, including the freedom of speech under the First Amendment of the U.S. Constitution.

<sup>18</sup> See generally, Stephen Breyer, *THE COURT AND THE WORLD* (Alfred A. Knopf 2015) at pp. 255-56.

<sup>19</sup> Compare, EU Commission Comment for NTIA, at 5.

amount to presumptively condoning the failed self-regulation policies that have increasingly undermined the trust of individuals on the web to the detriment of ecommerce and converging norms of cross border data flows.<sup>20</sup> Individual control is especially crucial as a pillar of the emerging new framework for the security and privacy of sensitive data.

#### B. Governance Over Previously Collected PII Retroactively

Today, the FTC should be empowered to lead as a catalyst to promote sound data protection and regulatory enforcement for the near, medium, and long term. The FTC should urge Congress to expressly confer upon it the role and duty to correct *retroactively* a myriad of misconduct stemming from the past accumulation and amalgamation of PII.

The wide range of misconduct that afflicts consumer privacy subsumes injurious practices that arise in both regulated industries and unregulated ones. These suspicious practices include many of the current PII collections and transfers on the periphery, or in the shadows, of regulated industries. Indeed, Big Data, Social Networks, and Information Technology providers often exploit past practices for amassing voluminous data. Many data controllers and processors lack any consumer contact at all, much less any opt-in evidence. New safeguards ought to be required now to end any further related actual or potential abuses, particularly under pretexts of a data broker's ownership of PII.

One underlying rationale for backwardly extending the FTC's power to govern such collections of PII retroactively could be a clear presumption against every data collector and processor that operate without any available showing of each person's opt-in. This rationale could render a reasonable inference that nearly all data brokers, except ones with opt-ins for a described limited purpose, likely acquired PII based upon an implicit subsidiary promise to the subject individual to permit his or her resumption of control over the PII. Data controllers and processor should be obliged to satisfy a duty to act in accordance with all FTC directives issued on behalf of individuals, including ones based upon each individual's ownership, access, and resumption of control of PII. The FTC could then suspend any continuing or further "secondary purpose" usage of any PII of an individual by a data broker until the latter attains each individual's express, specific, direct, and unambiguous consent and retains a record of it for audits.

---

<sup>20</sup> See Tim Wheeler, The Federal Trade Commission will safeguard privacy in name only, Brookings Papers, Nov. 28, 2018. (Calling the FTC out not only for "waffling" on safeguards in its own recent comments for the NTIA, but also expressing shock and awe over the FTC's disingenuous sleight of hand to relegate "the 'opt-in' privacy protections to become an 'opt-out' of advertising!" The FCC's former chief also added that "[t]he fundamental concept that the consumer should have the right to opt-in control of information collected about them magically transformed into opting out of advertisements."

### C. The FTC's Role As Consumer Privacy Court of First Instance

Augmenting *ex ante* regulations of data protection via rulemaking and *ex post* enforcement under a modernized framework are essential to close the regulatory gap that has been exacerbated by rapid technological changes. It is equally crucial for Congress to enable the FTC to exercise enforcement jurisdiction over precedential complaint cases as a court of first instance, with its final rulings subject to Appellate Review.

The FTC's conventional reliance predominantly upon settlements using the consent decree process still fails to build a corpus of precedential decisions that adequately facilitate legal certainty under *stare decisis*.<sup>21</sup> As a result, the deficiency in the predictable binding force of law remains troubling. Without a mandate for broader authority by the FTC to enforce data protection via quasi-judicial regulatory complaint proceedings, FTC enforcement power will remain diluted and suboptimal.

Under the status quo, companies continue to rationalize away their misconduct and self-dealing because no predictable application of the law or reasonableness standards have been authoritatively and lucidly described in advance. The FTC should urge Congress to empower it to instead proactively curb violative conduct by formalizing FTC complaint decisions that provide ample notice of rules and standards, so as to anticipate future defenses based upon hollow claims of legal uncertainty, unduly vague determinations, or distinguishable case-by-case resolutions. The FTC also should be empowered to leverage the doctrine of the private attorney general against big data operators as needed to curb unauthorized secondary uses of PII, as well to permit injured parties to recover statutory damages as well as attorneys' fees where appropriate.

The marketplace alone will not regulate itself effectively to protect PII. It is therefore critical at this time for Congress to imbue the FTC with the power to establish rules that leverage the FTC's decades of experience in privacy law. The FTC rulings could then iteratively level the playing field for Americans and most European stakeholders alike, even if certain limited sets of domestic exceptions to data protection in the U.S. are justifiable and proportionate. The FTC could leverage its newly delegated authority to also revitalize the influential guidance of its recent consent decrees on data privacy, data security, and data protection standards.

---

<sup>21</sup> In LabMD, *infra* at note 11, the Appellate Court explained the FTC's options for bringing claims of unfair acts or practices either administratively as in that case or in federal court as in FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D. N.J. 2014), *aff'd*, 799 F. 3d 236 (3rd Cir. 2015), and then evaluated the FTC's options for proceeding against a party that violates an order arising from either kind of case.

Where greater risks exist, the FTC ought to impose still higher levels of protection including fiduciary duties on data-intensive service providers and their information technology suppliers.<sup>22</sup> Even absent new authority, under the extant fairness prong, other clarifications are needed to:

- (a) define what data security standards are required by reference to a specified standard that is continuously revised at least quarterly.
- (b) control undue discriminatory pricing and treatment;
- (c) deter unconscionable acts that impair dignity with strict liability; and
- (d) end the misuse of collateral data to inferentially link PII sources.

Businesses need authoritative guidance in taking precautionary risk-based measures for data privacy and for data security as to technical, physical, and administrative safeguards.

#### 4. The FTC's Jurisdiction Should Be Clarified To Include Cross-Referencing

As Justice Breyer explained "the rise of problems that ignore national boundaries has made it necessary for the Court even more frequently to consider matters of international law and the law of other nations."<sup>23</sup> The FTC must follow the same cues as the Court and FTC authority should expressly permit referencing of the data protection laws of other advanced nations, and particularly ones under democratic governments.<sup>24</sup>

Equally important, the FTC's role encompasses an obligation to level the playing field of the protection of PII by substantially affording Americans nearly the full panoply of fundamental data protection rights substantially equivalent to that level of protection which the GDPR affords rights to Europeans, with only certain limited exceptions.

Like the EU, which has addressed the extraterritoriality of the scope of the GDPR,<sup>25</sup> U.S. reforms in enabling legislation and new binding rules must also advance a new approach to comity with the EU and the rest of the world. Even though some of the

---

<sup>22</sup> Accordingly, the instant comments request the FTC to urge Congress to confer extended authority to the FTC to exercise regulatory enforcement power over the data privacy compliance duties of large or high-volume data brokers, common carriers, communication providers, edge network companies, data-intensive operators, social networks, advertisement platforms, and data miners, as well as their suppliers of deployable information technologies and software.

<sup>23</sup> S. Breyer, *THE COURT AND THE WORLD*, *infra* at note 18, at 237.

<sup>24</sup> *Id.* at 236-246, but see, *Thompson v Oklahoma*, 487 U.S. 815, 868 n.4 (1988)(J. Scalia dissenting)(in his dissent, Justice Scalia urged that the pluralities' reliance upon what "other countries" do "is totally inappropriate as a means of establishing the fundamental beliefs of this Nation."

<sup>25</sup> See, e.g., European Data Protection Board (edpb), Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation, adopted on 16 November 2018.

terms may differ,<sup>26</sup> that new approach should, on balance, prevent the dilution of privacy safeguards in the face of burgeoning data flows and vital trade. Unlike nations that the EU designates as having satisfied its adequacy scrutiny, the U.S. and its companies must instead adapt their data protection measures to qualify to continue EU-U.S. data flows or PII under a transfer mechanism condoned under EU law.<sup>27</sup> The U.S. presently relies upon EU transfer mechanisms for some U.S. entities, provided that they qualify using Standard Contractual Clauses, Binding Corporate Rules, or the Privacy Shield option.<sup>28</sup>

Under the principle of subsidiarity, policy decisions are to be made at the lowest level appropriate for the decision. That principle, of course, indicates that global matters require governance under international law. Yet, as we have seen in the past, not every matter that entails cross-border interests or cooperation is politically ripe for unified rule-making under international law, and often the optimal outcome that can be achieved will only arise through substantive legal convergence or conflicts of law rules.

#### 5. Convergence in Consumer Privacy Via U.S. Conflicts of Law Rules

The plurality of nations relies upon differing systems of data protection law and privacy regulation. The pluralist regulation of cross-border conduct and data-driven services by national governments can result in conflicts of national regulations.<sup>29</sup> Referencing in advance of conflicts by U.S. authorities can minimize these conflicts whenever more than one nation has a colorable basis to exert prescriptive jurisdiction.

If a cause of action contains a foreign element, private international law identifies the conditions under which the court is competent to entertain the claim.<sup>30</sup> Decades ago,

---

<sup>26</sup> See, e.g., T. Shaw, When should a DPO bail out of their contract (June 26, 2018)(differentiating between separate EU rights of privacy and data protection, in view of Articles 7 and 8 of the European Charter of Human Rights and subsequent secondary legislation).

<sup>27</sup> The history of external transfers from the EU and the interplay between "adequacy" status and other EU transfer mechanism has been aptly summarized elsewhere by others. See e.g., Comments of Privacy Scholars to NTIA, *infra* at note 1, at 45-48.

<sup>28</sup> On October 6, 2015, the Court of Justice of the European Union (CJEU) invalidated the Safe Harbor program in a decision on the Maximilian Schrems v Data Protection Commissioner case (C-362-14). In Schrems, the CJEU construed the adequacy standard to require "essentially equivalent" and not identical data protection in a foreign regime. Schrems, [2015] E.C.R. I-\_\_\_\_, ¶ 74. See generally SIDLEY AUSTIN LLP, ESSENTIALLY EQUIVALENT: A COMPARISON OF THE LEGAL ORDERS FOR PRIVACY AND DATA PROTECTION IN THE EUROPEAN UNION AND UNITED STATES (2016), <http://www.sidley.com/~media/publications/essentially-equivalent---final.pdf>

<sup>29</sup> See generally, P.M. North & J.J. Fawcett, PRIVATE INTERNATIONAL LAW 3-4 (Buttersworth 12th Ed. 1992).

<sup>30</sup> *Id.* at 2-1. Often, an exercise of prescriptive jurisdiction may engender greater deference by other nations of interest, if the party who is subject of that exercise has clearly had reasonable

Professor Maier presciently observed that "[o]nly a state with a relationship to the activities giving rise to a cause of action should be able to prescribe the rules that will regulate the consequences of those activities."<sup>31</sup> Still, nearly a different regime of private international law exists for every nation and every nation may weigh differently a party's acts, intent, and effects, as well as the forum's own judicial goals.

A. Private International Law May Identify The Applicable Law

Unlike the past century, this century promises to more commonly enable individuals to enforce their data protection rights against those who violate them either within their jurisdiction of residence or abroad. The U.S. can no longer legislate in disregard of those direct rights, nor act in ways oblivious to those shared interests and the norms of nations. The FTC and the Courts will soon have recurring opportunities to consider whether to decide some data protection cases that implicate U.S. conflict of law rules in a way that favors convergence with the norms of the GDPR or with the laws of other foreign nations.<sup>32</sup>

Likewise, the U.S. does not conduct commerce dependent upon data flows in some kind of walled-garden or vacuum, but acts rather as a leading partner with other nations and companies in world or bilateral trade. Absent common rules, it is generally "the function of Private International Law to determine which of several simultaneously valid [national] legal systems is applicable to a given set of facts."<sup>33</sup> One observer has noted that:

"[e]ach nation, however, has its own 'private international law' that includes conflict of law rules that set the norms of jurisdiction, choice of law, and enforcement standards. A nation's conflicts of law rules are potent because they may override and supplant that nation's otherwise applicable laws. As nations apply their laws and rules in cyber-disputes,

---

actual or constructive notice of the law's applicability and if the law is interpreted not inconsistently with the law of nations.

<sup>31</sup> Harold G. Maier and Thomas R. McCoy, A Unifying Theory for Judicial Jurisdiction and Choice of Law, *Am. J. of Comp. L.* 249, 255 (Spring 1991)

<sup>32</sup> See also, S. Breyer *THE COURT AND THE WORLD*, *infra* at note 18 at 92-93. Justice Breyer says that lawmakers increasingly ask three salient questions paraphrased as follows: (1) To what extent does American law govern activities that relate to data protection that take place abroad in large part? (2) To what extent must courts take account of foreign law and related practices when interpreting the reach of an American statute? (3) How is our set of domestic statutes best interpreted to work together with those law and practices of other nations that also seek to enforce data protection norms?

<sup>33</sup> See, Martin Wolff, *PRIVATE INTERNATIONAL LAW* 5 (Oxford 1951);

the must strive to improve certainty and predictability throughout the global administration of justice rather than to fragment it."<sup>34</sup>

States often use different approaches in considering foreign law and factual elements, or use similar approaches but find that they yield disparate results.

#### B. Conflicts of Law Rules are National in Character

In the U.S., jurists may ask: would "it be reasonable for an American court to exercise jurisdiction over these foreign parties and their conduct, or would it not?"<sup>35</sup> Our courts and tribunals can apply domestic conflicts of law rules to determine whether U.S. or foreign law should apply in a data protection proceeding and reach a conclusion at odds with another state, even after making reference to the foreign law of that state.<sup>36</sup> Unlike Treaty law, conflicts of law rules have been national in character.

Traditionally, our domestic courts usually decided a civil case according to the law in the "place of the wrong", or *lex loci delicti*. In an era of cloud computing, big data, and transnational data flows that, however, the place of the wrong might be any of the nations that have a rational link to the activity, occurrence, parties, processing facilities, or transaction. There is not necessarily a distinct or exclusive *lex loci delicti*.

Justice Breyer acknowledged, however, that the Supreme Court "no longer seeks only to avoid direct conflicts among laws of different nations: it seeks, rather to harmonize the enforcement of what are often similar national laws."<sup>37</sup> Still, this hardly produces a paragon of predictability in an already murky area like consumer privacy law; but there is an array of analytical tools that may permit more rigorous guidance. These tools, which often presuppose cross-referencing, may be vital to address how to regulate the PII of businesses that are often made up of networks, or connected divisions located across borders, each of which "reacts to and plans with the others second by second."<sup>38</sup>

---

<sup>34</sup> S. Hoffer, *WORLD CYBERSPACE LAW* 1-2 (Juris Publishing 1999)

<sup>35</sup> S. Breyer, *THE COURT AND THE WORLD*, *infra* at note 18, at 103,

<sup>36</sup> Yet, in the U.S. a "court will not enforce a judgment if 'the cause of action on which the judgment was based, or the judgment itself, is repugnant to the public policy of the United States or the State where recognition is sought.'" See *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 433 F.3d 1199, 1213-14 (9th Cir. 2006) (en banc)(quoting RESTATEMENT (THIRD) of FOREIGN RELATIONS LAW OF THE UNITED STATES §482(2)(d)(1987); see also, RESTATEMENT at §483.

<sup>37</sup> S. Breyer, *THE COURT AND THE WORLD*, *infra* at note 18, at 96; see also, *Id.* at 99 (citing *Timberlane Lumber Co. v. Bank of Am.*, 549 F.2d 597, 614 (9th Cir. 1979)(adumbrating seven key points for "interest-balancing" under a multifactor approach).

<sup>38</sup> See, *Id.*; see also, *Hartford Fire Ins. Co v. California*, 509 U.S. 764, 817 (1993)(Scalia, J., dissenting ("The 'comity' [*Timberlane* and related cases] refer to is not the comity of courts, ... but

The U.S., like some other nations, remains internally divided over the proper tests used to determine the relevant category of case or applicable law.<sup>39</sup> As such, some of the best guidance can be gleaned, instead from four of the leading U.S. Supreme Court cases, and their progeny, that help delimit proper exercises of prescriptive jurisdiction.<sup>40</sup>

Under Private International Law "connecting factors" are facts or links, which tend to connect the occurrence, transaction, or status of an individual with a particular law or jurisdiction. Some common connecting factors include without limit the location of an injury, the domicile or residence of a person, the nationalities of adversely effected class of persons, the place of performance of a contract, and the targeted contacts of a business defendant of one nationality within another jurisdiction.

Absent common legal frameworks, sometimes the common denominators of private international law, namely connecting factors and categories (of cases), are used inconsistently among nations. This results in conflicts between conflict rules. Such conflicts of conflict rules usually arise in one of three main ways noted below.<sup>41</sup>

---

rather what might be termed 'prescriptive comity': the respect sovereign nations afford each other by limiting the reach of their laws.")

<sup>39</sup> Some U.S. courts, instead, apply a "center of gravity" approach, "comparative impairment" analysis, or a "better rule of law" test. Yet, many courts may simply apply forum law, *lex fori*.

<sup>40</sup> F. Hoffmann-La Roach Ltd. v. Empagran, S.A., 542 U.S. 155, 159 (2004); Advanced Micro Devices, Inc. v Intel Corp., 542 U.S. 241 (2004); Morrison v. Nat'l Austl. Bank Ltd, 561 U.S.247 (2010); and Kitsaeng v. John Wiley & Sons, Inc., 133 S.Ct. 1351, 1356 (2013).

<sup>41</sup> First, there may be a conflict as to the proper connecting factor, which is when conflict rules may differ on their faces. For instance, in a cross-border claim that entails the alleged unauthorized secondary use of an individual's PII, the individual's national court may assert that the proper forum is the *place of performance* of the contract that required the initial data use, namely at the state where the defendant is domiciled, while the national court in the defendant's domicile might find the proper forum to be *where the act caused harm* outside the contract, namely in the individual's state of residence.

Second, the conflict rules may both rely on the same connecting factor, but the two nations interpret it differently. For instance, in the first fact example, even if both forums viewed the case as governed by the law of the forum where the contract was performed, one could view the law of the proper forum law to coincide with the place where the first use of the data was authorized, while another could interpret it as another forum where the last use may have been justified under legitimate interest rationale.

Third, there may be total accord that the same connecting factor would apply to a given category of data protection cases like contract cases in the first example, but a conflict arises over whether a case falls within that category or one on unlawful contracts against public policy in a different forum. Compare, Hoffer, *World Cyberspace Law* 4-2 (1999).

## 6. Conclusion

The Privacy Without Borders Organization, at [privacywithoutborders.org](http://privacywithoutborders.org), is a nascent public interest organization dedicated to advancing the data privacy interests of under-represented stakeholders through the investigation of privacy laws and the study of data protection regulations worldwide. Despite the divisions among nations, a fresh look at this time may only deepen the FTC's analyses toward a better societal outcome. One approach is “harmonizing up” to the “better rule of law” to advance effective protection towards privacy without borders. It would lead toward the elevated protection of consumer privacy on the basis of the rule of law, democracy, equality, and justice. It would also deflect the brunt of the privacy injuries from unduly befalling upon Americans, especially ones who have neglected to actively opt-out of advertisements, by transforming the Fair Information Privacy Principles to substantially protect Americans equally with citizens of other advanced democracies.