Cross-Border Commerce without Constraint: Shifting from Territorial-Based Regulation to an Industry-Based Code of Conduct for the Online Payment Processing Industry*

Anna Myers**

TABLE OF CONTENTS

I. OVERVIEW 436

II. OPPS AND THE DATA SECURITY REGULATION LANDSCAPE ... 440

A. Online Payment Processors and Cross-Border Data Transfers *441*

B. Territorial-Based Regulation Models *441*

1. United States Regulation of OPPs 442
2. International Regulation 444

C. Industry-Based Self-Regulation Models *448*

1. The Fair Information Practice Principles (FIPPs) 449
2. Network Advertising Initiative 450
3. The PCI Data Security Standard and Security Standards Council 451

III. DATA SECURITY REGULATION, OF OPPS NEEDS TO SHIFT AWAY FROM TERRITORIAL-BASED REGULATION AND TOWARDS INDUSTRY-BASED REGULATION. 453

*****This note was submitted for publication on April 8, 2014. The Asian-Pacific Economic Commission (APEC) finalized a certification scheme for information processors during August 2015. The scheme, APEC Privacy Recognition for Processors (PRP) is corollary to APEC's Cross-Border Privacy Rules (CPBR), for more information visit the CPBR website, http://www.cbprs.org/. *See* APEC Privacy Recognition for Processors Ready for Implementation, Hunton Privacy Blog (Sept. 8, 2015), https://www.huntonprivacyblog.com/2015/09/08/apec-privacy-recognition-processors-ready-implementation/.

******J.D., The George Washington University Law School, 2015; B.A. in Rhetoric and Media Studies, Willamette University. The author would like to thank her life-long mentor, Dr. Mary Jo Myers, M.D.

A. Government Regulation is Ineffective Because it is Limited by its Territorial Jurisdiction, Which is Contrary to the Structure and Boundaries of the Internet Commerce Facilitated by OPPs. An Industry-Based Code of Conduct is the Solution to Today's Interconnected World. *454*

B. OPPs Should Merge and Adapt Self-Regulation Models Employed by Other Industries to Construct an Industry Code of Conduct. *454*

1. An OPP code of conduct should have clearly defined principles specific to the OPP industry. 456
2. An OPP code of conduct should be flexible enough to take advantage of advancements in technology. 457
3. An OPP code of conduct should be enforceable. 458

IV. CONCLUSION 459

I. OVERVIEW

News of a data breach[1] during the last shopping days of the year can be devastating for a company. Target announced a massive data breach on December 19, 2013 that compromised up to 40 million customers' payment information from purchases made between November 27 and December 15, 2013.[2] Reports of similar data breaches at other U.S. retailers, such as at Neiman Marcus and Michaels Stores, continued to make headlines into the New Year.[3] Breaches like these are not easy to recover from, financially and otherwise, costing banks the credit and debit card replacements, costing consumers their personal information, and costing the breached businesses the resulting damages, including their customers' trust. It is no wonder Target offered 20% off at their brick-and-mortar stores to salvage what holiday sales they could in the wake of their breach.

When only one company suffers a breach it may be because that company somehow failed to follow industry best practices for data security.[4] However when large U.S. retailers are falling victim to breaches one after

1. A data breach occurs when sensitive, protected, or confidential information is accessed by a hacker or disclosed through an error by the company or agency storing the information. Definition: Data Breach, TECHTARGET.COM, http://searchsecurity.techtarget.com/definition/data-breach (last updated May 2010).

2. Melanie Eversley & Kim Hjelmgaard, *Target Confirms Massive Credit-Card Data Breach*, USA TODAY, Dec. 19, 2013, http://www.usatoday.com/story/news/nation/2013/12/18/secret-service-target-data-breach/4119337/.

3. *See* Elizabeth A. Harris et al. , *Neiman Marcus Data Breach Worse Than First Said*, NEW YORK TIMES, Jan. 23, 2014, http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html; Nicole Perlroth, *Michaels Stores Is Investigating Data Breach*, NEW YORK TIMES, Jan. 25, 2014, http://www.nytimes.com/2014/01/26/technology/michaels-stores-is-investigating-data-breach.html.

4 . Additionally companies may be subject to compulsion by the United States Government to share the information they store. The USA PATRIOT Act and Foreign Intelligence Surveillance Act (FISA), under the premise of preventing espionage or terrorism, allows the United States Government to engage in warrantless, domestic surveillance programs and to order telecom and Internet companies to provide data in relation to national security investigations. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001); *see also* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511 92 Stat. 1783 (1978) [hereinafter *FISA*]. Without the protection of an Anti-hacking bill, companies are required to share the information they hold on their users with the government while also being accountable to their users for sharing that information; an Anti-Hacking Bill designed to provide protection from liability for companies that share information with the government was delayed because of the Snowden Leaks. Chris Strohm, *Anti-Hacking Bill Aiding Verizon Delayed by Snowden Leaks*, BLOOMBERG POLITICS (June 28, 2013, 12:01 AM ET), http://www.bloomberg.com/news/2013-06-28/anti-hacking-bill-aiding-verizon-delayed-by-snowden-leaks.html.

the other it signals a greater problem within the industry: that the current standards employed by businesses to prevent breaches are not working.[5]

While abstinence from data collection is the only absolute protection currently[6] – if there is no data there is nothing to breach – eliminating all data collection is not a realistic option for retailers in today's information age.[7] The data businesses collect feed essential operations, such as processing payments and providing customer service.[8] Liability can be minimized in some industries, such as the advertising industry, by limiting the data collected to less sensitive types of information.[9] Retailers, however, often use third-party payment processors to serve as middlemen in a transaction to collect and process financial information so the retailers do not have to face the liability associated with collecting that information.[10] The payment processors bear the liability[11] for the sensitive data they need to collect to operate effectively.[12]

During the sales process the collected information is used to verify the identity of the purchaser, verify that the payment method is authentic, and

---

5. Nicole Perlroth, *Experts Find a Door Ajar in an Internet Security Method Thought Safe*, N.Y. TIMES, Apr. 8 2014, http://bits.blogs.nytimes.com/2014/04/08/flaw-found-in-key-method-for-protecting-data-on-the-internet.

6. There is always a risk of a breach no matter how well data is secured or how much is invested in data security. "You can never completely stop attackers from accessing data because there's a lot of clever tricks they can play…(Encryption is) like locking your front door (to deter burglars), but there are other ways in." Jessica Morris, *Yahoo Announces Latest Move in Privacy Battle*, CNBC, (Apr. 3, 2014, 10:31AM), http://www.cnbc.com/id/101551972.

7. BUSINESS WITHOUT BORDERS: THE IMPORTANCE OF CROSS-BORDER DATA TRANSFERS TO GLOBAL PROSPERITY, U.S. CHAMBER OF COMMERCE AND HUNTON & WILLIAMS LLP 6 (2014), https://www.huntonprivacyblog.com/files/2014/05/021384_BusinessWOBorders_final.pdf.

8. Data Security, FTC, http://www.business.ftc.gov/privacy-and-security/data-security (last visited Apr. 8, 2014)

9. *See generally* UPDATE TO THE 2015 NAI CODE OF CONDUCT, NETWORK ADVERTISING INITIATIVE (2015), http://www.networkadvertising.org/sites/default/files/NAI_Code15encr.pdf. Types of information listed from least to most sensitive: anonymous, pseudonymous, personally identifiable information (PII), and sensitive PII.

10. For example, PayPal allows users to send and receive payments without sharing financial information with the other transacting party, whether the purchaser or the seller. PAYPAL, ABOUT PAYPAL, https://www.paypal-media.com/about (last visited Mar. 4, 2014).

11. Stewart Room, *The Privacy Regulatory Bear Market and Playing Political Football with Business*, PRIVACY & INFO. L. BLOG (Jan. 23, 2014), http://privacylawblog.ffw.com/2014/the-privacy-regulatory-bear-market-and-playing-political-football-with-business.

12. "The ready availability of personal information helps businesses 'deliver the right products and services to the right customers, at the right time, more effectively and at lower cost.'" Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 882 (2000) (quoting Fred Smith, founder and President of the Competitive Enterprise Institute at the time).

verify the necessary funds are available for the purchase.[13] Collecting that information, however, makes payment processors a target for hackers. Akin to the Target breach, Heartland Payment Services, Inc., a payment processor, suffered a breach in 2009 that compromised as many as 100 million payment card records.[14] Similarly, online payment processors (OPPs), such as PayPal, collect financial information, such as a credit card number, expiration date, and verification code, to process purchases and authorize sales online.[15] E-commerce is valued at an estimated $8 trillion per year[16] – which equates to more than ten-percent of the Gross World Product.[17] While commerce is increasingly conducted online via cross-border data flows,[18] "merchants, financial institutions, and consumers all still have substantial concerns about the security of online payments . . . and the privacy of personal information."[19]

Data protection standards should aim to limit possible data breaches, the resulting damages from any breaches, and simultaneously to limit the liability of companies when they are the non-offending party. Under current data-breach regulations, financial institutions – including banks, payment processors, and OPPs – bear the liability for a breach of any information they collect, even when they are not the offending party.[20] Data breach notification laws vary by state, but they all assign liability through an indirect liability regime.[21] This indirect liability regime punishes the OPP or payment intermediary, which are already victims of the data breach, instead of punishing the actions of the actual bad actor: the hacker.[22]

Hackers can be difficult to punish because technology can obscure the hacker's identity and true location.[23] An IP address is regarded as a weak identifier to serve as evidence in a criminal case that a particular individual carried out an activity, such as illegal downloading, because an IP address

---

13. *See id* at 882-884.

14. Mark McCarthy, *Information Security Policy in the U.S. Retail Payments Industry*, 2011 STAN. TECH. L. REV. 3, ¶ 60.

15. About PayPal, *supra* note 10.

16. *Business Without Borders*, *supra* note 7, at 5.

17. World GDP (Official Exchange Rate) estimates the Gross World Product (GWP) at $74.31 trillion (2013), http://www.indexmundi.com/world/gdp_%28official_exchange_rate%29.html.

18. Joshua Meltzer, *The Internet, Cross-Border Data Flows and International Trade*, BROOKINGS.EDU (Feb. 25, 2013), http://www.brookings.edu/research/papers/2013/02/25-internet-data-flows-international-trade-meltzer.

19. ESTHER C. RODITTI, 3-11A COMPUTER CONTRACTS § 11A.01 , at 1 (Matthew Bender & Co. 2013), LEXIS.

20. McCarthy, *supra* note 14, at ¶ 34.

21. *Id.* at ¶ 20.

22. *See id*.

23.*See* VPR Int'l v. Does 1-1017, No. 11-2068, 2011 U.S. Dist. LEXIS 64656 at *4 (C.D. Ill. Apr. 29, 2011) (finding that IP address provided by ISP did not accurately identify illegal downloader).

merely identifies the location where a certain activity occurred.[24] A hacker's true location though can sometimes be found through online geo-location tools that can collect more information than just a hacker's location.[25] That collected data can be aggregated at times to sufficiently identify an individual.[26] OPPs, however, should not be liable just because the true criminal may be difficult to find; instead OPPs should be held to high standards that if met limit their liability in the case of a data breach.

The current data protection regime is not effective at limiting possible data breaches or OPP industry liability when a hacker gains unauthorized access to data.[27] In contrast, other legal regimes such as copyright law give OPPs a safe-harbor when third parties use OPPs to commit illegal acts.[28] For example, when distributors use an OPP to sell copyright infringing work, OPPs are not liable for those sales because OPPs do not make a material contribution to infringement by processing those sales.[29] Similarly, if OPPs meet sufficiently high data protection standards they should not be liable for unauthorized access by a hacker.

Data management compliance for OPPs is complex, costly, and ineffective because the laws are constantly evolving and still do not alleviate the concerns of merchants, financial institutions, or consumers.[30] OPPs are currently regulated under a traditional territorial-based approach, with regulations applying at the state, national, and international levels.[31] At the state level, each state has its own data breach notification law, at the national level there is no national standard for data breach notification,[32] and at the international level, multiple countries have laws specific to data security practices within their borders.[33] Outside of formal regulations, countries and

---

24. *See In re* BitTorrent Adult Film Copyright Infringement Cases, 296 F.R.D. 80, 84-5 (E.D.N.Y. 2012). A computer in a household is usually shared, which means a child, a boyfriend, or any other visitor, is just as likely to be using the computer. *See id.* Many households now have a wireless network and if the network is not secured others may use an IP address without the original account holder's knowledge. *See id.*

25. *See* Jerusha Burnett, Note, *Geographically Restricted Streaming Content & Evasion of Geolocation: The Applicability of the Copyright Anti-Circumvention Rules*, 19 MICH. TELECOMM. & TECH. L. REV. 461, 484 (2013).

26. *See id.* at 483.

27. *See* McCarthy, *supra* note 14, at ¶ 34.

28. *See* Perfect 10, Inc. v. Visa Int'l Serv. Assoc., 494 F.3d 788, 795-96 n.4 (9th Cir. 2007).

29. *Id.*

30. Roditti, *supra* note 19, at 1.

31. McCarthy, *supra* note 14, at ¶ 12; *Business Without Borders: supra* note 7, at 14.

32 . Security Breach Notification Chart, PERKINS COIE, revised Oct. 2013, http://www.perkinscoie.com/statebreachchart/.

33. "Such inconsistency. . . saddles businesses with the cost of identifying which data protection regime applies to a given act of data processing, understanding the requirements of that regime, and then applying them appropriately, and the risk of liability if they fail to reconcile inconsistent data protection requirements appropriately. The problem is especially true online. The Internet crosses state and national boundaries and has facilitated truly global markets. . .The price of inconsistent data protection laws is borne by entities that must comply

international organizations promulgate general guidelines.[34] These guidelines consist mainly of lists of basic information practice principles that are too broad to apply to specific industries, are unenforceable, and lack consensus. This traditional approach has proven to be an ineffective approach to cyber regulation because it fails to adapt to online, globally connected networks.[35]

Data security regulation, especially for the OPP industry, needs to shift away from territorial-based regulation and towards industry-based regulation. This shift is best achieved for OPPs through an industry-specific code of conduct, because it encourages active participation by industry members to develop industry standards and best practices; it can be implemented more quickly than regulation; it is flexible enough to be applied internationally and nationally; it is flexible enough to adapt to changing technologies; and it takes into account the business and technological capabilities of OPPs.

First, this note provides more in-depth information on OPPs, the current territorial-based regulatory landscape for OPPs, and models of industry-based regulatory systems from other industries that should be used to create an industry code of conduct for OPPs. Second, this note analyzes the reasons behind the need for a shift away from territorial-based regulation and towards industry-based systems. Lastly, this note constructs the basics of an OPP industry code of conduct from a combination of self-regulation industry models.

II. OPPS AND THE DATA SECURITY REGULATION LANDSCAPE

The OPP regulatory landscape is challenging for several reasons. First, OPPs are unique because of the sensitive information they need to collect to run their business. Without information identifying the individual initiating a transaction and the relevant financial information, an OPP would be unable to process a payment. Second, the current regulation surrounding OPPs is territorial-based which does not reflect the global nature of online commerce. Third, self-regulation industry-based models used by other industries could be used by OPPs to address the data security challenges of their industry and to construct a code of conduct for the OPP industry.

---

with those laws and by individuals whose privacy is supposed to be protected by them." Fred H. Cate, *The Failure of the Fair Information Practice Principles in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 368-69 (Jane K. Winn ed., Ashgate Pub. Ltd. 2006), http://ssrn.com/abstract=1156972.

34. *Id.* at ¶ 13.

35. "Looking at the bigger picture of privacy law enforcement, penalties and sanctions, the climate has been getting worse for businesses year-on-year … [t]he regulatory rhetoric getting stronger and darker over the cycle…[with the] imposition of large financial penalties and negative rhetoric in press statements, television appearances and promulgation of guidance and policy documents." Room, *supra* note 11.

A. Online Payment Processors and Cross-Border Data Transfers

OPPs process online payments using information provided by the purchaser(s) to validate financial information. For example, OPPs based in the United States collect credit card information to authorize a transaction such as the credit card number, cardholder name, expiration date, billing address, and the Card Verification Value (CVV) number from the back of a credit card.[36] The collected information is then transmitted, using the account number for routing, to the appropriate bank that either authorizes or denies the transaction based on the authenticity of the information provided.[37] The CVV is a primary means of authorization and is used as an access code that if entered correctly indicates to the bank that the cardholder is initiating the transaction and access to the related account is authorized.[38] Internationally, other countries use chip and PIN technology; the authentication process is similar, but instead of using a CVV, a new authentication code is used for each transaction to reduce the risk of fraud.[39] Similarly, PayPal provides a security option for consumers to have a security code sent to their mobile device each time they log onto their account or use PayPal in a transaction.[40] OPPs, through those authentication processes, facilitate cross-border transactions that grow the global economy.[41]

B. Territorial-Based Regulation Models

Existing regulations surrounding OPPs are primarily based on political territories, meaning that the laws applying to OPPs vary from country to country, ignoring the modern reality that online transactions occur across borders and across the globe. On a global scale there is a lack of clarity of which jurisdiction a company is subject to (or should be subject to), or what list(s) of international guidelines a company should follow. The interconnected world calls for a release from this territorial-based regulation

36. McCarthy, *supra* note 14, at ¶ 27.

37. *Id.* at ¶ 24.

38. *Id.*

39. *Id.* at ¶ 26.

40 . PAYPAL, PAYPAL SECURITY KEY, https://www.paypal.com/us/webapps/mpp/security/security-key (last visited Mar. 3, 2014).

41. *Sotto Speaks on the Importance of Cross-Border Data Transfers to Global Prosperity*, PRIVACY & INFO. SEC. L. BLOG (May 20, 2014), https://www.huntonprivacyblog.com/2014/05/articles/sotto-speaks-importance-cross-border-data-transfers-global-prosperity/.

because it is limited in its reach, applicability, and ability to protect information.[42]

1. United States Regulation of OPPs

In the United States, data breach notification law is regulated at the state level (there is currently no national data-breach notification standard), and OPPs are primarily regulated indirectly through standards developed to apply to financial institutions, such as banks and the payment card industry.[43] Attempts to create data protection standards at the national level by the United States Congress have failed. In 2005 Senator Patrick Leahy (D-VT) introduced the Personal Data Privacy and Security Act.[44] The bill sought to *inter alia* require notice of security breaches, increase protections against security breaches, and enhance criminal penalties for security breaches.[45] Senator Leahy has reintroduced the bill in each Congress since 2005 and it has failed to pass each time.[46] On January 8, 2014, Senator Leahy reintroduced the bill again.[47] That version of the bill again proposes a national standard for data breach notification, criminal penalties for intentionally concealing breaches that cause economic damage to consumers, and requirements that businesses protect sensitive customer information from cyber threats by implementing internal data protection policies.[48] The bill additionally contains provisions that explicitly grant authority to the Federal Trade Commission (FTC) to create and enforce rules requiring companies to protect personally identifiable information and to

42. "Because location has less meaning in an electronic world, protecting privacy requires attaching protection to the … record itself, rather than to the institution that generates it." Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 513 (1995).

43. Eunice Chung et al., *Consumer Data Protection In Online Retail: On Protecting Privacy in the EU, US, and China*, DLA PIPER RE:MARKS ON COPYRIGHT & TRADEMARK (Nov. 17, 2014), http://www.remarksblog.com/internet/consumer-data-protection-in-online-retail-on-protecting-privacy-in-the-eu-us-and-china/.

44. Personal Data Privacy and Security Act of 2005, S.1789, 109th Cong. (2005) (related bill S. 1332 introduced on June 29, 2005), https://www.govtrack.us/congress/bills/109/s1789.

45.*See id.*

46. *See e.g.*, *Senators Renew Efforts to Pass Data Privacy Legislation*, PRIVACY & INFO. SEC. L. BLOG (Jan. 13, 2014), https://www.huntonprivacyblog.com/2014/01/articles/senators-renew-efforts-pass-data-privacy-legislation/; Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007) (reintroduced as S. 1490 on July 22, 2009); Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009) (reintroduced as S. 1151 on June 7, 2011); Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011) (reintroduced as S. 1897 on Jan. 8, 2014).

47. Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014), https://www.govtrack.us/congress/bills/113/s1897.

48. The bill also includes a provision requiring the Computer Fraud and Abuse Act to be updated to make attempted computer hacking and conspiracy to commit computer hacking punishable under the same criminal penalties as the underlying offense. *See id.*

notify customers of a breach.[49] However, given the bill's legislative record it is unlikely it will pass without more significant amendments from prior versions of the bill proposed in previous Congressional sessions and suffers from the inability to apply on an international level.

The United States House of Representatives' version of a data-breach notification bill, the Data Accountability and Trust Act (DATA), also has a poor legislative record. First introduced in 2007, the House bill failed all three times it was introduced (and reintroduced) by Congressman Bobby Rush (D -Ill.).[50] In 2009, DATA, which aims to eliminate the confusion and cost in meeting multiple states regulations for breach notification procedures, passed the House but not the Senate.[51] If DATA had passed, it would have superseded existing state laws for data breach notification[52] – essentially creating a federal data breach notice process.[53] Once again, such a law would be limited in its reach to United States territory.

Specifically, the Gramm-Leach-Bliley Act requires financial institutions, which indirectly includes service providers such as OPPs[54] to adopt information security programs to protect consumer information.[55] The

---

49. Currently the FTC exercises authority over data security through section 5 of the FTC Act's prohibition on unfair or deceptive acts or practices. *See* FTC v. Wyndham Worldwide Corp., 2013 U.S. Dist. LEXIS 41494 (D. Ariz. Mar. 25, 2013); LabMD, Inc., FTC Docket No. 9357, *dismissal denied* Jan. 16, 2014; *see also* FTC, 2014 PRIVACY & DATA SECURITY UPDATE (2014), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

50. Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007) (reintroduced as H.R. 2221 on Apr. 30, 2009), https://www.govtrack.us/congress/bills/110/hr958. Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009), (reintroduced as H.R. 1707 on May 4, 2011), https://www.govtrack.us/congress/bills/111/hr2221. Data Accountability and Trust Act, H.R. 1707, 112th Cong. (2011), (reintroduced as H.R. 1707 on May 4, 2011), https://www.govtrack.us/congress/bills/111/hr2221.

51. H.R. 2221, *supra* note 50.

52. States are largely opposed to federal regulation that would supersede their local laws. States want to maintain their own rules because of fears that the national standard will be weaker than their own rules and to preserve their authority to enforce data breach regulations. Jessica Meyers, *States Defend Turf from Feds on Data Breach Rules*, POLITICO (Feb. 19, 2014), http://www.politico.com/story/2014/02/states-defend-turf-from-feds-on-data-breach-rules-103647.

53. Richard E. Mackey, Jr., *Understanding the Data Accountability and Trust Act*, INFO. SEC. (Dec. 2010), http://searchsecurity.techtarget.com/magazineContent/Understanding-the-Data-Accountability-and-Trust-Act.

54. MacCarthy, *supra* note 14, at ¶ 45. Counter intuitively, service providers are requested to "store transaction data much longer than needed for billing purposes in order to facilitate criminal investigations." *See* Sarah Spiekermann & Lorrie Faith Cranor, *Engineering Privacy*, 35 IEEE Transactions on Software Engineering, no. 1, January/February 2009, at 72, http://ssrn.com/abstract=1085333.

55. 15 U.S.C. § 6801(a). More specifically, 16 C.F.R. § 314.4 explains the necessary elements of an information security program. *See* FTC, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT: A GUIDE FOR SMALL BUSINESS FROM THE FEDERAL TRADE COMMISSION (July 2002),

Act requires multiple agencies, including the FTC, Comptroller of the Currency, and the SEC to establish "appropriate standards for the financial institutions subject to their jurisdiction," "to insure security and confidentiality of customer records and information" and to "protect against unauthorized access" to the information.[56] The Act and other United States laws all have the same flaw – they do not account for the global nature of online commerce and are limited in their reach and enforceability by territorial jurisdiction.

Challenges to data protection for trans-border data flows cannot be solved with isolated regulations promulgated by individual countries focused on the location of the data sender, receiver or processor.[57] In addition to the territorial limits on the reach of government regulations, "[i]t is difficult to see how broad or comprehensive new privacy laws or regulations at the present time could keep pace with the revolutionary and extraordinarily rapid transformation of the Internet and other new media technologies."[58] Location, geographic-based legislation is limited in its effectiveness, inconsistent, costly, fails to incorporate industry expertise, and impedes cross-border data flows necessary for modern business.[59]

2. International Regulation

Currently there is no international standard for data protection and "[t]he situation only grows worse as more states and nations develop inconsistent data protection laws with which they attempt to regulate increasingly global information flows."[60] Existing regulation varies by country, with each country using different scales[61] to balance privacy rights[62] and the free flow of information.[63] Guidelines that do apply at the international level consist mainly of lists of basic information practice

---

http://www.business.ftc.gov/documents/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.

56. 15 U.S.C. § 6801(b).

57. Joel R. Reidenberg, *Symposium: Electronic Communications and Legal Chance: Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6 HARV. J. LAW & TECH. 287, 290 (1993).

58. Wendy Davis, *Ad Groups Tout Self-Regulation to White House*, THE DAILY ONLINE EXAMINER (Apr. 1, 2014), http://www.mediapost.com/publications/article/222759/ad-groups-tout-self-regulation-to-white-house.html#reply (quoting the Association of National Advertisers).

59. Ira Rubenstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 ISJLP 356, 361 (2010).

60. Cate, *supra* note 33, at 344.

61. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 155-56 (2004).

62. Nader v. General Motors Corp., 255 N.E.2d 765, 772 (N.Y. Ct. App. 1970) (Brietel, J. concurring).

63. Cate, *supra* note 12, at 884.

principles that are too broad to apply to specific industries, are unenforceable, and lack consensus. Even within the European Union (EU), conflicting provisions impede "the ability of computer users in the European Union to transfer computerized information across national borders."[64]

The EU, Malaysia, Brazil, Mexico, the Netherlands, and France[65] all are working on creating or revising their existing data protection regulations, joining the close to 100 countries already with individual data protection statutes.[66] Proposed and current regulations aim to simultaneously meet the needs of multiple industries and balance the competing goals of privacy protection and the free flow of information.[67] Even under the slim possibility that the laws from these 100 countries integrate harmoniously to create a global web of data protection regulation,[68] the ability to create a cohesive understanding of all the regulations (much less comply with them) is a daunting and costly task for any business. While OPPs face the challenge of meeting this myriad of international data protection regulations, countries in turn struggle to design regulations that meet the needs of their citizens, are broad enough to cover multiple industries, and simultaneously are narrow enough to be enforceable.[69]

For example, Brazil recently proposed a requirement that domestic and international companies who collect data related to Brazilian citizens store

64. Amy Fleischmann, Note, *Personal Data Security: Divergent Standards in the European Union and the United States*, 19 FORDHAM INT'L L.J. 143, 150 (1995) (noting as an example when the French Government prohibited the transfer of Fiat's employee information from Italy because it considered Italian data security requirements inadequate).

65. In fact, the Netherlands and France are subject to their own data protection regimes as well as the overlapping EU regulations. For example, the French Data Protection Authority (CNIL) adopted new guidelines on processing bank card details related to the sale of goods and services at a distance in response to the increase in online transactions. Olivier Proust, *CNIL Issues New Guidelines on the Processing of Bank Card Details*, PRIVACY & INFO. L. BLOG (Feb. 27, 2014), http://privacylawblog.ffw.com/2014/cnil-issues-new-guidelines-on-the-processing-of-bank-card-details.

66. Phil Lee, *2013 a Big Year for Privacy? You Ain't Seen Nothing Yet!*, PRIVACY & INFO. L. BLOG (Dec. 31, 2013), http://privacylawblog.ffw.com/2013/2013-a-big-year-for-privacy-you-aint-seen-nothing-yet.

67. "Data privacy rules are often cast as a balance between two basic liberties: fundamental human rights on one side and the free flow of information on the other side. Yet, because societies differ on how and when personal information should be available for private and public sector needs, the treatment and interaction of these liberties will express a specific delineation between the state, civil society, and the citizen." Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1341-42 (2000).

68. DLA Piper provides a comprehensive and interactive tool on the varying state of data protection laws around the globe. *See Data Protection Laws of the World*, DLA PIPER, (Paul McCormack & Kate Lucente, eds.), http://www.dlapiperdataprotection.com (last visited Mar. 5, 2014).

69.Reidenberg,, *supra* note 57, at 290.

that data physically on servers in Brazil.[70] This localization effort received criticism from organizations across the globe[71] because it would have the consequence of forcefully subjecting companies to Brazil's data protection law if they do business with Brazilian citizens.[72] Additionally, companies attempting to avoid the law would face the choice of complying with its requirements, or limiting their business to customers outside of Brazil.[73] It is unclear how the nationality or physical location will affect how the law impacts the collection of personal information by a corporation. Does the law apply to anyone physically located within Brazil, regardless of their nationality? If a company collects information on a Brazilian citizen while they are traveling abroad, is the law valid, or is its application limited solely to Brazilian citizens while they are located on Brazilian soil?

Brazil has since dropped the local data storage rule from the proposed bill, but it still states that global Internet companies, including financial services such as OPPs,[74] "are subject to Brazilian laws in cases involving information on Brazilians even if the data is stored abroad."[75] This could have a chilling effect on global business especially as other countries follow in Brazil's footsteps[76] and extend the reach of their laws to businesses that collect information on their citizens.[77] Even without the local storage rules, such legislation hinders the growth of the global economy because it forces

---

70. Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill*, WALL ST. J. (NOV. 13, 2013, 6:45 PM ET), http://online.wsj.com/news/articles/SB10001424052702304868404579194290325348688.

71. Letter from the Global Business Community to Members of the Brazilian Congress in re Data Center Localization (Oct. 22, 2013), http://www.wilsoncenter.org/sites/default/files/Data%20Center%20Localization%20-%20English%20version.pdf.

72. *See* Chao, *supra*.

72. *See* Chao, *supra*.

73. *See* Chao, *supra* (stating that companies that don't comply could be "barred from doing business in one of the world's most significant markets or be obligated to pay millions of dollars in fines).

74. "In-country data requirements threaten to harm Brazil's competitive and global automotive, its manufacturing and service industries, like aerospace, oil and gas, financial services, retail, and healthcare industries and also R&D operations." *Id.*

75. *Brazil Removes Local Data Storage Requirement from Internet Bill*, PRIVACY & INFO. SEC. L. BLOG (Mar. 19, 2014), https://www.huntonprivacyblog.com/2014/03/articles/brazil-removes-local-data-storage-requirement-internet-bill/.

76. *Russian Parliament Adopts Internet Privacy Bill Requiring Data Localization*, PRIVACY & INFO. SEC. L. BLOG (July 7, 2014), https://www.huntonprivacyblog.com/2014/07/articles/russian-parliament-adopts-internet-privacy-bill-requiring-data-localization/; HUNTON & WILLIAMS LLP, *Deadline for Compliance with Russian Localization Law Set for September 1, 2015*, PRIVACY & INFO. SEC. L. BLOG (Jan. 2, 2015), https://www.huntonprivacyblog.com/2015/01/articles/deadline-for-compliance-with-russian-localization-law-set-for-september-1-2015/.

77. Phil Lee, *Challenges in Global Data Residency Laws – and How to Solve Them*, PRIVACY L. BLOG (Sept. 13, 2014), http://privacylawblog.fieldfisher.com/2014/challenges-in-global-data-residency-laws-and-how-to-solve-them.

companies to choose to comply with Brazilian (or the propagating country's) law or to limit the geographic reach of their business.[78]

International data protection standards, embodied in multiple lists of guidelines, are beneficial in providing education and resources on improving data protection; however, these guidelines have failed to bring unity to European data security requirements.[79] The high level at which the guidelines were developed provides a theoretical framework, not a practicable one. First, the guidelines do not supersede existing data security requirements.[80] Second, the guidelines cannot be enforced on an international level without universal adoption by all countries and a body to enforce the guidelines.[81] Finally, global standards are too broad to meet the needs of multiple groups with differing needs and capabilities and are challenging to apply to any specific issues, industries, or types of information.[82]

For example, in 2013 the Organization for Economic Cooperation and Development (OECD) updated the privacy guidelines it originally promulgated in 1980.[83] The guidelines outline the need for a practical, risk management-based approach to implementing privacy protection, enhanced privacy protection on a global level through interoperability, national privacy strategies, privacy management programs, and for global standards for notification following a data security breach.[84] The revised guidelines make suggestions for the protection of privacy and trans-border flows of personal information, highlighting the challenge to create international standards. International standards created through guidelines however lack the enforceability of regulations or legislation.[85] Additionally the guidelines are

78. "Thus, in-country data storage requirements would detrimentally impact all economic activity that depends on data flows." Letter from the Global Business Community, *supra* note 71.

79. Herald D.J. Jongen & Gerrit A. Vriezen, *The Council of Europe and the European Community*, *in* DATA TRANSMISSION AND PRIVACY 140-55, 150 (Dennis Campbell & Joy Fisher eds., 1994).

80. Alexander D. Roth, *Introduction to Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 19 I.L.M. 282, 282 (1980).

81. For example, The German Data Protection Authority (DPA) published its own recommendations for mobile payment services. HUNTON & WILLIAMS LLP, *German DPA Publishes Recommendations for Mobile Payment Systems*, PRIVACY & INFO. SEC. L. BLOG (Nov. 13, 2013), https://www.huntonprivacyblog.com/2013/11/articles/german-dpa-publishes-recommendations-mobile-payment-systems/.

82. Reidenberg Symposium, *supra* note 57, at 290.

83. OECD, GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (July 11, 2013), http://www.huntonprivacyblog.com/wp-content/uploads/2013/09/2013-oecd-privacy-guidelines.pdf.

84. *See generally id.*

85. *OECD Issues Updated Privacy Guidelines*, PRIVACY & INFO. SEC. L. BLOG (Sept. 16, 2013), http://www.huntonprivacyblog.com/2013/09/articles/oecd-issues-updated-privacy-guidelines/.

meant to apply on a large scale, "at the highest level of government," and so are too broad to provide effective protection for online consumers.[86]

Industry-focused data management standards for OPPs therefore could help synthesize the myriad regulations, guidelines, and recommendations into understandable and applicable principles that are specific to the needs of the industry and would be easier for the OPP industry to implement.[87]

C. Industry-Based Self-Regulation Models

Government agencies such as the Department of Commerce and the FTC favor self-regulation in the privacy arena because it is more flexible, cost-effective, and can keep pace with technological advancement.[88] The United States additionally recognizes the validity of self-regulation through safe-harbor programs in copyright law, under the COPPA rule, and in the Online-Based Advertising industry.[89] An effective safe-harbor program combines the advantages of a flexible self-regulatory code with the enforcement power of a governmental body. However, safe-harbor programs suffer from the same scalability challenge that territorial-based regulation does because it is unclear how consistent application of the standards can occur on the international scale without an international 'governmental' body to vest with enforcement power. While safe-harbor framework exists for some cross-border data transfers,[90] "sectors not regulated by the FTC, such as financial services, telecommunication common carriers, and insurance, are not covered by the Safe Harbor Frameworks."[91] Therefore an

86. *Id.*

87. "Information about individuals' needs and preferences is the cornerstone of any system that allocates goods and services within an economy." *Federal Privacy Issues: Hearing Before the Subcomm. on Fin. Insts. & Consumer Credit of the Comm. on Banking and Fin. Servs*,.106th Cong. (1999) (testimony of Fed. Reserve Bd. Governor Edward Gramlich), http://www.federalreserve.gov/boarddocs/testimony/1999/19990721.htm.

88. Rubenstein, *supra* note 59, at 356.

89. Perfect 10, Inc. v. Visa Int'l Serv. Ass'n., 494 F.3d 788, 795 n.4 (9th Cir. 2007); *FTC Acts on Several Industry COPPA Proposals*, PRIVACY & INFO. SEC. L. BLOG (Mar. 14, 2014), https://www.huntonprivacyblog.com/2014/03/articles/ftc-acts-several-industry-coppa-proposals/; ADVERTISING SELF-REGULATORY COUNCIL, SUNTRUST BANK REFERRED TO THE CFPB FOR REFUSAL TO PARTICIPATE IN SELF-REGULATION (May 8, 2014), http://www.asrcreviews.org/2014/05/suntrust-bank-referred-to-the-cfpb-for-refusal-to-participate-in-self-regulation/.

90. *Business without Borders*, *supra* note 7, at 21. "The Safe Harbor framework is composed of a set of Privacy Principles and Frequently Asked Questions. To certify to the Safe Harbor, organizations generally are required to (1) conform their privacy practices to the Safe Harbor Privacy Principles; (2) file a self- certification form with the Department of Commerce; and (3) publish a Safe Harbor privacy policy that states how the company complies with the Privacy Principles."

91. Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, *at 33, The White House, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (last visited July 3, 2012).

independent self-regulation model is necessary for financial services such as OPPs.

Three primary industry-based models created by other organizations and industries are useful for creating a code of conduct for the OPP industry. First, the Fair Information Practice Principles (FIPPs) are an appropriate starting point for any data collection system, because they are principles agreed upon by the United States and a number of European Countries through privacy agreements and national laws.[92] Second, the Network Advertising Initiative's code of conduct models a successfully implemented voluntary code of conduct in the third-party online advertising industry. Third, the Payment Card Industry's (PCI) Data Security Standard is relatable to, and can be adapted for, the OPP industry.

1. The Fair Information Practice Principles (FIPPs)

The eight FIPPs "are the benchmark against which the FTC and privacy advocates evaluate any self-regulatory privacy scheme," and are used by the private and public sector as a basis for their privacy and data collection policies.[93]

> **1. Transparency**: information collectors should be transparent in their collection, use, dissemination, and maintenance practices.
> **2. Individual Participation**: consent of the individual for the collection of the data should be obtained.
> **3. Purpose Specification**: the specific purpose(s) the information is being collected for should be articulated.
> **4. Data Minimization**: only the information necessary to accomplish the specified purpose should be collected.
> **5. Use Limitation**: the information should only be used for the specific purpose(s) for which it is being collected.
> **6. Data Quality and Integrity**: To the extent practicable collected information should be accurate, relevant, timely, and complete.
> **7. Security**: Collected information should be protected from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

---

92. The FIPPs are the core of the Privacy Act of 1974, are adopted by the Department of Homeland Security as its policy framework, and are the root of the OECD privacy guidelines. *See* HUGO TEUFEL III, U.S. DEP'T OF HOMELAND SEC., MEMO. NO. 2008-01, PRIVACY POLICY GUIDANCE MEMORANDUM 2-4 (Dec. 29, 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

93. Rubenstein, *supra* note 59, at 382; *see also,* Appendix B to the White House's 2012 Privacy Report includes a table demonstrating the continuity of the FIPPs through the Consumer Privacy Bill of Rights, the OECD Privacy Guidelines, the DHS Privacy Policy, and the APEC Principles. Consumer Data Privacy, *supra* note 91, at 49.

> **8. Accountability and Auditing**: Collecting organizations should be accountable for compliance with the FIPPs and the use of information should be audited to demonstrate compliance with the FIPPs and all applicable data protection requirements.[94]

A data collection practice assessed under the FIPPs is analyzed for the methods used to achieve each FIPP, the barriers to achieving each FIPP, the risks and impacts in the system to achieving each FIPP, and any compensating controls or measures that can mitigate those risks and impacts. In some cases, not all of the FIPPs are applicable to a given system.[95]

2. Network Advertising Initiative

The Network Advertising Initiative (NAI) developed a code and mobile code of conduct based on the FIPPs as well as additional principles for the online third-party advertising industry.[96] NAI is essentially a trade association of third-party online advertisers that voluntarily adhere to its code.[97] NAI's code is based on the FIPPs outlined above and serves as an example of how those principles can be adapted to a particular industry.[98] While membership in the NAI is voluntary, prospective members must achieve compliance with the NAI code before being granted membership and all existing members must maintain compliance with the code.[99] The NAI received criticism at its start for four primary reasons: (1) the NAI opt-out cookie did not work consistently; (2) the NAI had a static approach to self-regulation which was not flexible enough to emerging technologies or the varying business models of ad networks; (3) the NAI self-regulation model did not include a majority of groups within the behavioral advertising industry; and (4) the enforcement program lacked transparency and independence.[100]

Despite initial setbacks, the NAI is now recognized for its robust compliance and enforcement program and NAI's 2013 compliance report demonstrates how its strict self-regulatory code can be effectively used to protect data privacy and honor consumer choices.[101] In 2013, 3.9 million

---

94. Descriptions of FIPPs adapted from Privacy Policy Guidance Memorandum, *supra* note 92, at 3-4.

95. *Id.*

96. About the NAI, http://www.networkadvertising.org/about-nai/about-nai (last visited Mar. 5, 2014).

97. NAI Code of Conduct, at 1, http://www.networkadvertising.org/2013_Principles.pdf (last visited Mar. 5, 2013).

98. *Id.* at 3.

99. *Id.* at 1-2, 8.

100. *Id.*

101. *NAI Achieves Highest Level of Member Compliance in Consumer Privacy*, THE MAKEGOOD (Apr. 8, 2014), http://www.the-makegood.com/2014/04/08/nai-achieves-highest-

consumers used NAI's opt-out mechanism to opt-out of tracking by NAI member ad networks.[102] NAI's membership represents "a significant portion of the marketplace" with 88 member ad networks in 2013.[103] NAI membership additionally includes the largest ad networks such as Google, Yahoo, AOL, and Microsoft and all members must comply with the strict standards of NAI's code of conduct.[104] NAI's code of conduct is more easily updated than regulation, because the code can be revised as frequently as necessary to reflect technological changes. For example, NAI's updated 2014 code of conduct requires ad-networks to use opt-in consent for sexual orientation[105] and its mobile code of conduct recognizes "that maintaining an effective Mobile Application Code may require, at least initially, regular iterations, with full notice and participation by stakeholders."[106]

3. The PCI Data Security Standard and Security Standards Council

More closely related to OPPs, the Payment Card Industry (PCI) developed a Data Security Standard in 2004 and an independent Security Standards Council (PCI SSC)[107] in 2006 to manage the standard.[108] The PCI wanted a "truly industry-wide standard, administered by an entity independent of the particular card companies that originally developed the standard."[109] Similar to the FIPPs, the PCI standard is conceptualized by

---

level-of-member-compliance-in-consumer-privacy/; *see also* Katy Bachman, *Report: Ad Networks Adhering to Strict Privacy Guidelines* (Mar. 13, 2014) (quoting NAI CEO, Marc Groman) http://www.adweek.com/news/technology/report-ad-networks-adhering-strict-privacy-guidelines-156277.

102. *Id.; contra* Wendy Davis, *Ad Groups Tout Self-Regulation to White House*, (Apr. 1, 2014) ("[I]t's not practical for consumers to try to 'turn off' the data machine . . . [t]here have to be regulatory rules that limit the collection of data and empower individuals to make their own privacy decisions.") (quoting the Center for Digital Democracy), http://www.mediapost.com/publications/article/222759/ad-groups-tout-self-regulation-to-white-house.html#reply.

103. Katy Bachman, *Report: Ad Networks Adhering to Strict Privacy Guidelines* (Mar. 13, 2014) (quoting NAI CEO, Marc Groman), http://www.adweek.com/news/technology/report-ad-networks-adhering-strict-privacy-guidelines-156277.

104. *Id.*

105. *Id.*

106 . 2013 NAI Mobile Application Code (2013), http://www.fcclaw.com/wp-content/uploads/2013/08/LNGS-Mobile-Payments-Network-Advertising-Initiative-2013-Mobile-Application-Code-2013-08-02.pdf.

107. PCI SSC was created by American Express, Discover Financial Services, JCB, MasterCard, and Visa. McCarthy, *supra* note 14, at ¶ 40.

108. *Id.*

109. *Id.*

basic requirements with more detailed sub-requirements. The PCI standard has twelve basic requirements:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.[110]

The PCI requirements, however, were designed to meet the business needs of payment card companies such as Visa and therefore do not meet the needs of OPPs.[111] PCI members store financial information for different purposes than OPPs.[112] PCI members store financial information to maintain financial accounts for their customers.[113] The types of information PCI members need to maintain financial accounts include the account holder's name, billing address, email address, and phone number, a record of every transaction made using the account, the account balance or credit limit.[114] Essentially PCI members collect and store information related to a customer's account to create a comprehensive financial record for the customer's account. Maintenance of a customer's account requires storing this data for the duration of the life of the account.[115]

While the PCI standard applies directly to members of the PCI, such as MasterCard and Visa, they apply indirectly to OPPs who are considered "service providers" to the Payment Card Industry.[116] The PCI standard applies indirectly to service providers by requiring that members only do

110. *Id* at ¶ 41.
111. *Id* at ¶ 40.
112. *See id.*
113. *See id.*
114. *See id.* at ¶¶ 40-41.
115. *See id.* ¶ 41.
116. *Id.* at ¶¶ 40, 45.

business with PCI-compliant service providers.[117] OPPs, however, only need financial information for the duration of processing a transaction. The data storage requirements under the PCI standard should not be applied to OPPs in the same way they are applied to PCI members, because it requires OPPs to store and maintain payment information beyond the time required to process a payment. Once the transaction is processed, the information is no longer needed by the OPP and OPPs should not be compelled to unnecessarily store and maintain sensitive payment information in order to do business with the PCI. For example, OPPs should instead destroy the payment information once the transaction is completed so that it is not vulnerable to hackers. Requiring PCI members and their service providers to store and maintain payment information duplicates the locations in which payment information can be found. The less locations payment information can be found, the less chance that information will be compromised. Therefore the standards applicable to PCI members should not unilaterally apply to their service providers because it creates greater risk of a data breach. Instead OPPs should be regulated by standards tailored to the business processes and needs of the OPP industry.[118]

III. DATA SECURITY REGULATION, OF OPPS NEEDS TO SHIFT AWAY FROM TERRITORIAL-BASED REGULATION AND TOWARDS INDUSTRY-BASED REGULATION

OPPs should adopt international standards through an industry specific code of conduct because it is a proven solution that meets the modern needs of global-based businesses and economies in ways that territorial-based regulation fails. The code should concern itself not with *where* data is processed but *why* it is processed and *how* it is protected.[119] First, international standards for data security should be based on the business needs of specific industries rather than the physical location of a piece of data to accurately reflect the global nature of modern commerce. Second an

117. *Id.* at ¶ 45.

118. "If sound rules for the use of personal data are not established and enforced, society as a whole will suffer because people will decline to engage in a range of different social interaction due to concerns about use of personal information." Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2089 (2004).

119. "So long as data is kept secure and processed in accordance with the controller's legal obligations and in keeping with its data subjects' reasonable expectations, it should be free to process that data wherever in the world it likes. Maintaining unrealistic restrictions on international data exports at best achieves little—organizations will do it any way using check-box solutions like model clauses—and, at worst, will adversely impact critical technology developments like the cloud." Phil Lee, *What a 21st Century Privacy Law Could – and Should - Achieve*, IAPP PRIVACY PERSPECTIVES, (Jan 20, 2014), https://www.privacyassociation.org/privacy_perspectives/post/what_a_21st_century_privacy_law_couldand_shouldachieve.

industry standard should be adopted through an industry code of conduct based on other successful self-regulation industry models.

A. Government Regulation is Ineffective Because it is Limited by its Territorial Jurisdiction, Which is Contrary to the Structure and Boundaries of the Internet Commerce Facilitated by OPPs. An Industry-Based Code of Conduct is the Solution to Today's Interconnected World

In the past territorial-based laws made sense because "norms of privacy in fact vary considerably from place to place, culture to culture, period to period."[120] The laws protecting individuals reasonably reflected the cultural values and norms of an individual's nationality. Political borders were a natural legal boundary because of the location-based nature of criminal activity before the Internet globalized society as well as crime. The rapid interconnection facilitated by the Internet globalized communities and globalized the way services are provided and business is conducted. "When self-regulation works effectively, it's a win for consumers and industry and regulators that have limited enforcement resources." [121] A regulation structure that accounts for the international nature of modern commerce is needed because "the boundaries of networks are defined by technological protocols and network infrastructure, not by physical geography."[122] Rather than being built on the basis of the culture and values of each country, the code should be built to meet the needs of the industry and be specific to the type of data being collected.[123]

B. OPPs Should Merge and Adapt Self-Regulation Models Employed by Other Industries to Construct an Industry Code of Conduct

In combination the three industry-based models, the FIPPs, the NAI Code of Conduct, and the PCI Data Security Standard can be used to create

120. Nissenbaum, *supra* note 611, at 155-56.

121. Katy Bachman, *Report: Ad Networks Adhering to Strict Privacy Guidelines* (Mar. 13, 2014) (quoting NAI CEO, Marc Groman), http://www.adweek.com/news/technology/report-ad-networks-adhering-strict-privacy-guidelines-156277.

122. RODITTI, *supra* note 199, at 2.

123. "[N]ational laws are often incompatible, they often impose explicit barriers to the international flow of personal data, and they are increasingly supplemented by state, provincial, and even local data protection laws. As a result, data protection has grown inconsistent and unpredictable, and increasingly burdensome to multinational commerce, trade, and information flows." Cate, *The Failure of the Fair Information Practice Principles*, *supra* note 33, at 367.

FIPP	Possible Interpretation[124]
Transparency	This principle is broadly applicable to all information collectors because it requires collectors to be transparent in their collection, use, dissemination, and maintenance practices. This transparency is often achieved through a company's privacy policy. OPPs should have a privacy policy that explains their privacy practices to the consumer and should be easily accessed for example through a link or displayed when requesting consumer information.
Individual Participation	This requirement is focused on the consent of the individual for the collection of the data. However, this is generally inapplicable to OPPs because consent of an individual is usually clear in a payment transaction. Consent of the individual providing the information is usually clear because the individual is providing the financial information specifically for the purpose of a transaction. In comparison, an individual browsing the web may be unaware that by conducting a Google search, the individual may be served advertisements based on the keywords they use in the search. OPPs should obtain consent for use of any information outside of the purpose of processing a transaction. See the Purpose Specification interpretation for more information.
Purpose Specification	The objective of this principle that the specific purpose(s) the information is being collected for should be articulated is also often achieved through a privacy policy. Additionally consent check boxes can be used for users to opt-in to allowing their data to be used for purposes beyond completing the transaction, for example being added to a mailing list to receive coupons from the seller.
Data Minimization	Data minimization is a significant principle that is not implemented as often as it should be. Ideally only the information necessary to accomplish the specified purpose should be collected and it should only be stored for the duration necessary to accomplish that specified purpose. OPPs would benefit from removing data from their systems after the necessary time to process a transaction.
Use Limitation	This principle is related to Purpose Specification. The difference is Purpose Specification is focused on providing notice to individuals about the purpose for which the information is being collected while Use Limitation addresses the actual use of the information. Information collected should only be used for the specific purpose(s) for which it is being collected and for which individuals have notice of its use. This is essential to a code of conduct for OPPs because they are required by United States law to only use the information collected to process the payment unless the individual manually consents to other uses for the information.
Data Quality & Integrity	This principle is core to the function of OPPs. The purpose of OPP data collection is to ensure the identity of the purchaser and the authenticity of the payment information. It is of high importance that the information OPPs collect is accurate, relevant, timely, and complete to the extent practicable.
Security	OPPs should protect collected information from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. In addition to a comprehensive security program, once again OPPs should

	only retain the information as long as necessary to complete the transaction.
Accountability & Auditing	This is the most important principle of the FIPPs because it provides the enforcement mechanism for the FIPPs. An OPP industry code of conduct should hold OPPs accountable for compliance with the code and OPPs should be audited to demonstrate compliance with the code's data protection requirements.

a comprehensive OPP industry code of conduct. There are three main goals for an OPP code of conduct. First, the code should be constructed with clearly defined principles specific to the OPP industry with additional commentary to explain the provisions of the code. Second, the code should be flexible enough to take advantage of advancements in technology. Finally, the code should be enforceable.[125]

1. An OPP code of conduct should have clearly defined principles specific to the OPP industry

The FIPPs are useful as a starting place to construct a code of conduct, but are broad and require interpretation based on a comprehensive understanding of OPP business processes. Using the FIPPs to help design the code can illuminate business processes that can also be helpful in protecting information, such as limiting the amount of data necessary for those processes and removing any unnecessary information once the transaction is complete. For example once the financial information has been verified the CVV may no longer be needed and once the transaction has been fully processed the remaining financial information is no longer needed. The following possible interpretation of the FIPPs serves as an example of how the FIPPs may be adapted to the OPP industry and the general applicability of each FIPP. The code created by the OPP industry should expand on and amend the suggested interpretations as necessary to reflect OPP business processes. The code should contain additional commentary to explain the

124. Interpretations of FIPPs for the OPP industry adapted from Privacy Policy Guidance Memorandum, *supra* note 923, at 3-4.

125. These three main goals for an OPP code of conduct track with the six critical elements for the success of a self-regulatory code identified by Ira S. Rubenstein: (1) efficiency - achieving regulatory objectives at the lowest attainable cost; (2) openness - whether the system allows public stakeholders to play a role in the development of the code – and transparency - regulatory system's ability to promulgate industry normative standards and provide information about the performance of member companies in meeting those standards; (3) completeness -code addresses all relevant aspects of standards governing industry practices; (4) Free rider problems – prevents members from enjoying the benefits of the program without having to meet its obligations; (5) oversight and enforcement – consumer complaint mechanism, routine audits, and consequences for failure to comply; and (6) Use of second-generation design features – reward members for superior performance. Rubenstein, *supra* note 599, at 381-83:

intent and provisions of the code, and to provide examples of ways members can meet the code.[126]

OPPs additionally should use the institutional knowledge about financial services offered by the PCI Data Security Standard to develop an OPP industry-specific code of conduct. However, the requirements of the PCI Data Security Standard should not apply directly to OPPs because it was designed with the business processes of bank card companies such as Visa and MasterCard in mind.[127] Instead the standards should be adapted to reflect the business processes of OPPs. Banks for example need to store information for longer periods of time – as long as a customer holds an account – and OPPs only need the information for as long as necessary to complete a given transaction. Some of that information such as the CVV value can be purged in the initial stages of that transaction once it has served its purpose.

2. An OPP code of conduct should be flexible enough to take advantage of advancements in technology

The code should include technical recommendations on equipment and practices that will help companies meet the code and should be flexible enough to take advantage of advancements in technology. Technological solutions can also help ensure industry compliance. For example, NAI has a tool that crawls the web to make sure companies are complying with their code.[128] Technical mechanisms similar to NAI's web tool can be used to perform daily auditing tasks and boost compliance with a code of conduct.[129]

In addition, the code should have technical standards to ensure the security and protection of information. Technology is rapidly advancing and data security standards that were previously thought to be secure are sometimes discovered to have flaws.[130] A code needs to be adaptable to these changes. For example, encryption technology could be used to simplify the payment authentication process and provide additional protections to

126. 2013 NAI Code of Conduct, at 9 (2013), http://www.networkadvertising.org/2013_Principles.pdf (last visited Mar. 5, 2014).

127. McCarthy, *supra* note 14, at ¶ 42.

128. About the NAI, http://www.networkadvertising.org/about-nai/about-nai (last visited Mar. 5, 2014).

129. Spiekermann & Cranor, *supra* note 544, at 73.

130. For example the SSL encryption key used to encrypt websites was recently discovered to have a flaw. Nicole Perlroth, *Experts Find a Door Ajar in an Internet Security Method Thought Safe*, NEW YORK TIMES, Apr. 8 2014, http://bits.blogs.nytimes.com/2014/04/08/flaw-found-in-key-method-for-protecting-data-on-the-internet.

consumer information. Further technological developments could allow for payment authentication with limited identifying information.[131] The industry code of conduct should be designed so it can be consistently revised to keep pace with such technological advancements.[132]

3. An OPP code of conduct should be enforceable

For the code to be effective, it needs to be enforceable and provide accountability for compliance with its provisions. A code is enforceable when it is enforced by a single enforcement body to ensure uniform interpretation of the code and when it has multiple methods of enforcement that analyze, track, and enforce compliance with the code.

First, the enforcement structure should include multiple methods of enforcement, because not all methods of enforcement are effective nor is any one method effective on its own. For example, codes that are enforced only when a company receives a complaint, investigates the complaint and finds the complaint valid require knowledge by consumers of the code and assertive action by those consumers.[133] This model lacks an auditing process for compliance. Audits for compliance should be conducted at regular intervals. The NAI code of conduct in particular demonstrates the impact a self-imposed code with real teeth can have as compared to a code created as a public relations move or window-dressing. A significant part of the success of the NAI code of conduct is its yearly compliance audits for its members.[134] Each year the NAI conducts a compliance audit of all of its members' activities and publicly publishes a compliance report.[135]

While useable as a model, NAI's code, like the PCI Data Security Standard, is not directly applicable to the OPP industry. NAI members are online advertisers that usually collect non-sensitive, anonymous data, while OPPs collect sensitive financial information. Therefore because NAI members and OPPs collect different types of information codes of conduct for each industry should reflect those differences.

Moreover, the goals of data collection for advertisers differ from the goals of OPPs. Advertisers are less concerned about actual identification of the consumer (by name, etc.) and more that the consumer is receiving

131. "By using anonymous or pseudonymous credentials that attest to the relevant fact rather than to a person's identity, secure transactions can take place outside the user sphere without the transfer of personal information." Spiekermann & Cranor, *supra* note 544, at 74.

132. "System designers should consider the extent to which users can remain unidentified during electronic transactions." Spiekermann & Cranor, *supra* note 544, at 74.

133. *NAI's Marc Groman on Setting and Keeping High Standards in Online Advertising*, THE MAKEGOOD (Jan. 6, 2014), http://www.the-makegood.com/2014/01/06/nais-marc-groman-on-setting-and-keeping-high-standards-in-online-advertising/.

134 . NETWORK ADVERTISING INITIATIVE, 2013 ANNUAL COMPLIANCE REPORT http://www.networkadvertising.org/2013_NAI_Compliance_Report.pdf.

135. *Id.*

advertising that reflects his or her interests. For OPPs the goal is exactly the opposite, it is already clear what the consumer wants – the item in his or her digital shopping cart – the question is whether the consumer is who he or she says they are and is therefore authorized to use the method of payment they offer. Consequently the focus in data collection for OPPs is informational accuracy, identification, and verification.

An additional difference is that consent is a large issue with advertisers, whereas consent in payment processing is usually apparent because a user provides consent for the information to be used to process the payment at the time of purchase.[136] A code created specifically for OPPs would need to reflect these differences with heightened data security standards to match the heightened sensitivity of the financial information collected.[137] Privacy solutions are not one-size fits all[138] and solutions should reflect the context and content of the information involved.[139]

IV. CONCLUSION

Online payment processors are specifically vulnerable to cyber-attacks because they collect personally identifiable information and sensitive financial information to facilitate online transactions. The regulation needs to shift from a territorial based model to an industry-based model that accounts for individual businesses' needs and the types of information they collect and maintain.

This objective is best achieved through a self-regulated industry code of conduct. The code of conduct should be based in sound principles, such as the FIPPS, adapted to the OPP industry, should be flexible to adapt to emerging technologies and varying business practices, and should be enforceable through a comprehensive enforcement program.

---

136. However making sure the information collected to process a payment is limited to that purpose is often confusing for consumers. For example, when after a purchase a consumer starts receiving advertising emails from the same company it made the purchase from.

137. "Different categories of data present different levels of risk." 2013 NAI Code of Conduct, *supra* note 1266, at 9; *see also* Bruce Morris, *Responsible Data Management and Maintaining Consumer Trust*, NAI (Apr. 17, 2014), http://www.networkadvertising.org/blog/responsible-data-management-and-maintaining-consumer-trust ("NAI Code also has higher standards for sensitive information such as financial data that can result in identity theft…").

138. 2013 NAI Code of Conduct, *supra* note 1266, at 3; FTC REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, 19-20 (2012); WHITE HOUSE REPORT, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 9 (2012).

139. *Id.* at 18.