DATA PRIVACY AND INDIVIDUALISM: AN EXAMINATION OF THE TRANSATLANTIC PRIVACY DIVERGENCE

Anthony Glosson | Law & Anthropology Term Paper | Final Draft | 12.03.2014

SYNOPSIS

Compliance costs resulting from a litany of EU data privacy regulations run into the billions of dollars yearly. Many of the EU's most costly restrictions, however, are wholly absent from U.S. law. This paper explores this discrepancy in light of U.S. and EU cultural differences along the individualism-collectivism index.

Specifically, this paper evaluates how two elements of privacy law have developed in the U.S. and in the EU. The element deals with the enforcement of privacy—that is, the means with which each jurisdiction enforces privacy. This paper suggests that differing tendencies toward individualism and collectivism have influenced the selection and application of privacy principles in the U.S. and the EU. Individualistic cultures should exhibit tendencies toward means of privacy regulation that leave the market minimally disturbed, while more collectivist cultures should exhibit more willingness to use disruptive regulatory measures. This paper applies that dichotomy to explain the fact that where U.S. regulations do exist, they generally eschew *ex post* government oversight of collected data in favor of ensuring *ex ante* consumer consent to the act of collection, while the inverse is true in Europe. The second element involves the interaction between free speech and privacy. This paper invokes the individualism-collectivism framework to explain the relatively more robust speech protections in the U.S., and conversely, the more robust privacy protections in the EU.

At the same time, this paper seeks to emphasize the limitations and assumptions inherent in its proposals and methodologies, including its definition of autonomy, its conception of property and information ownership, and circumstances in which its explanations may not be supported. Ultimately, this paper concludes that the available evidence is consistent with its theory that privacy law derives, at least in part, from cultural attitudes toward autonomy.

TABLE OF AUTHORITIES

Statutory Law

International Treaties & Agreements

Case Law

United States v. Jones, 132 S. Ct. 945 (2012)
Von Hannover v. Germany, 2004 ECHR 294
(European Court of Human Rights, June 24, 2004)
Wagner and J.M.W.L. v. Luxembourg 76240/01/458 (European Court of Human Rights 2007)

Secondary Sources

Abdullah Bozkurt, *Intimidation toward press on 'sub judice' rule*, Today's Zaman (Jan. 20, 2014)
Adam Thierer, *Is Privacy an Unalienable Right? The Problem with Privacy Paternalism*, Technology Liberation Front (Jan. 27, 2014)
Allen C. Johnston & Merrill Warkentin, *National Culture and Information Privacy: The Influential Effects of Individualism and Collectivism on Privacy Concerns and Organizational Commitment*, 1 Int'l Fed. Info. Processing Paper 88 (2009)
Alan Peslak, *Internet Privacy Policies: A Review and Survey of the Fortune 50*, 18 Info. Resources Mgmt. J. 29 (2005)
Andrea Peterson, *How a failed Supreme Court bid is still causing headaches for Hulu and Netflix*, Washington Post (Dec. 27, 2013)
Andrej Savin, *Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks*, Copenhagen Business School Faculty Repository 3-7 (last visited Nov. 15, 2014)
Anita L. Allen, *Unpopular Privacy: The Case for Government Mandates*, 32 Okla. City U. L. Rev. 87, 99 (2007)
Ann Cavoukian et al., *The Unintended Consequences of Privacy Paternalism*, Privacy & Information Comm. White Paper 3-4 (Mar. 05, 2014)
Avigail Eisenberg, *Individualism and Collectivism in Northern Politics*, 1 Brit. Colum. Pol. Studies Assoc. 6 (1995)
Barton Gellman & Ashkan Soltani, *NSA tracking cellphone locations worldwide, Snowden documents show*, Washington Post (Dec. 04, 2013)
Calvin R. Massey, *Hate Speech, Cultural Diversity, and the Foundational Paradigms of Free Expression*, 40 UCLA L. Rev. 103, 115 (1992)
Charles R. Taylor et al., *Attitudes toward Direct Marketing and Its Regulation: A Comparison of the United States and Japan*, 19 J. Pub. Pol. & Marketing 228, 230, 234 (2000)
Christopher Wolf & Winston Maxwell, *So Close, Yet So Far Apart: The Eu and U.S. Visions of A New Privacy Framework*, 8 ABA Antitrust Symp. 9 (Summer 2012)
Daniel J. Solove & Paul M. Schwartz, Information Privacy Law, 1109-1114 (4th ed. 2011)
Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1879, 1897 (2013)
Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L.Rev. 1880, 1894-95 (2013)
Debra B. Rosler, *The European Union's Proposed Directive for the Legal Protection of Databases: A New Threat to the Free Flow of Information*, 10 High Tech. L.J. 105, 109 (1995)
Der Spiegel, *Edward Snowden Interview: The NSA and Its Willing Helpers*, Der Spiegel (July 08, 2013)
Electronic Frontier Foundation, *Best Practices for Online Service Providers*, EFF.org (last visited Nov. 15, 2014)

Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of A Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049 (2000)

European Commission, *Summary of Act: Data protection in the electronic communications sector*, Europa.eu (last visited Nov. 15, 2014)

Fred H. Cate, *The Eu Data Protection Directive, Information Privacy, and the Public Interest*, 80 Iowa L. Rev. 431 (1995)

Fredrick Schauer, *The Exceptional First Amendment*, Harv. Univ. Faculty Working Paper Series (February 2005)

FTC, *Fair Information Practice Principles*, FTC.gov (last visited Nov. 15, 2014)

FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, FTC.gov (Mar. 2012)

Geert Hofstede, Cultures and Organizations, Software of the Mind: Intercultural Cooperation and its Importance for Survival 13-14 (1997)

Geng Cui et al., *Consumers' Attitudes toward Marketing: A Cross-cultural Study of China and Canada*, 20 J. Int'l. Consumer Marketing 81 (2008)

Geoffrey Wheatcroft, *Privacy, Libel and the Case of Dominique Strauss-Kahn*, Nat'l Interest (May 19, 2011)

Graham Pearce & Nicholas Platten, *Orchestrating Transatlantic Approaches* to. *Personal Data Protection*: *A European*. *Perspective*, 22 Fordham Int'l L.J. 2024, 2040-41 (1999)

Gregory Shaffer, *Globalization and Social Protection: The Impact of Eu and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 Yale J. Int'l L. 1, 13 (2000)

Guy E. Carmi, Di*gnity-the Enemy from Within: A Theoretical and Comparative Analysis of Human Dignity As A Free Speech Justification*, 9 U. Pa. J. Const. L. 957, 973 (2007)

Hogan Lovells, *EU and U.S. privacy proposals converge on principles, diverge on method*, Global Media & Communications Quarterly (Spring 2012)

Ilhyung Lee, *The Law and Culture of the Apology in Korean Dispute Settlement (with Japan and the United States in Mind)*, 27 Mich. J. Int'l L. 1, 15 (2005)

International Chamber of Commerce, *ICC UK Cookie Guide*, international-chamber.co.uk (Apr. 2012)

James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 1151 (2004)

Joy M. Sever et al., *IBM Multi-National Consumer Privacy Survey*, White Paper (Oct. 1999)

Jan-Benedict E.M. Steenkamp & Inge Geyskens, *How Country Characteristics Affect the Perceived Value of Websites*, 70 J. Marketing 136 (2006)

Katarzyna Celinska, *Individualism and Collectivism in America: The Case of Gun Ownership and Attitudes toward Gun Control*, 50 Sociological Perspectives 229 (2007)

Lance Whitney, *Google hit by more than 144,000 'right to be forgotten' requests*, CNET (Oct. 10, 2014)

Lt. Col. Chas. A. Repington, [*Untitled*], Wash. Times, (Nov. 19, 1922)

Lucian G. Conway et al., *Collectivism and Government-Initiated Restrictions: A Cross-Sectional and Longitudinal Analysis Across Nations and Within a Nation*, 37 J. Cross-Cultural Psych. 20, 28-34 (2006)

Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 Stan. Tech. L. Rev. 1, 28 (2001)

Markus Kemmelmeier et al., *Individualism and Authoritarianism Shape Attitudes Toward Physician-Assisted Suicide*, 29 J. Applied Social Psych. 2613 (1999)

Markus Kemmelmeier, *Individualism and Attitudes Toward Affirmative Action: Evidence From Priming Experiments*, 25 Basic and Applied Social Psych. 111 (2010)
Matthias Bauer et al., *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, 3 Eur. Cent. Int'l Pol. Paper 2 (2014)
McGarr Solicitors, *Sub Judice*, McGarr Blog (Jan. 24, 2007)

Megan Geuss, *Cops hid use of phone tracking tech in court documents at feds' request*, Ars Technica (June 20, 2014)
Mobile Marketing Association, *Mobile Marketing Association Releases Final Privacy Policy Guidelines for Mobile Apps*, Press Release (Jan. 25, 2012)
Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 Am. Bus. L.J. 413, 449 (2013)
OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Doc. C 58 (Oct. 1, 1981)
Olivia Solon, *Compliance with EU cookie law could cost the UK £10 billion*, Wired UK (Apr. 24, 2012)
Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 Ohio St. L.J. 1217, 1218 (2013)
Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev. 877, 894 (2014)
Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055 (2004)
Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2058 (2004)
Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 Harv. L. Rev. 1966 (2013)
Pew Research Center, *The American-Western European Values Gap*, Global Attitudes Project (Feb. 29, 2012)
Princely Ifinedo, *The Effects of National Culture on the Assessment of Information Security Threats and Controls in the Financial Services Industry*, 12 Int'l J. Electronic Bus. Mgmt. 82 (2014)
Randy E. Barnett, *A Consent Theory of Contract*, 86 Colum. L. Rev. 269, 271 (1986)
Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Geo. L.J. 2381 (1996)
Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 Geo. Wash. L. Rev. 1162, 1177 (2011)
Robert Gellman, *Fair Information Practices: A Basic History*, BobGellman.com (last visited Nov. 15, 2014)
Robert Lemos, *FBI director to citizens: Let us spy on you*, Ars Technica (Oct. 16, 2014)
Ron Shevlin, *In Banks We Mistrust*, Aite Group (Oct. 21, 2009)
Russia Today, *'Test it on Brits:' Snowden says GCHQ even worse than NSA,* RT (July 20, 2014)
Sandra J. Milberg et al., *Values, Personal Information, and Regulatory Approaches*, 38 Comms. of the ACM 65 (1995)
Sarah Andrews, *Protecting Privacy Through Government Regulation*, 2 Sedona Conf. J. 1, 7 (2001)
See Lawrence Lessig, Code and Other Laws of Cyberspace 142-43 (1999)
Stephan Gardner, *EU Justice Nominee Notes Data Protection, U.S.-EU Safe Harbor at Nomination*

Hearing, Bloomberg BNA (Oct. 6, 2014)
Stephen Gardbaum, *The Myth and the Reality of American Constitutional Exceptionalism*, 107 Mich. L. Rev. 391, 403-04 (2008)
Susan J. Brison, *The Autonomy Defense of Free Speech*, 108 Ethics 312, 339 (1998)
Thomas Varela & David Gauthier-Villars, *France Urges Restraint From Media, Politicians*, WSJ (May 18, 2011)
Tamara Dinev et al., *Privacy calculus model in e-commerce – a study of Italy and the United States*, 15 Eur. J. Info. Systems 389 (2006)
Tamara Dinev et al., User Attitudes toward Protective Technologies, 19 Info. Systems J. 391 (2009)
U.S. Dep't of Commerce, *U.S.-EU Safe Harbor Framework*, Export.gov (last visited Nov. 15, 2014)
U.S. Dep't of Commerce, *U.S.-EU Safe Harbor Guide to Certification*, Paper (June 16, 2013)
U.S. Dep't of Health and Human Servs., *Summary of the HIPAA Security Rule*, HHS.gov (last visited Nov. 15, 2014)
U.S. Nat'l Inst. Science & Tech., *Fair Information Practice Principles (FIPPs)*, NIST.gov (last visited Nov. 15, 2014)
Virginia Boyd, *Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization*, 24 Berkeley J. Int'l Law. 939, 960 (2006)
Walter B. Kennedy, *Law and the Railroad Labor Problem*, 32 Yale L.J. 553, 559 (1923)
Wolters Kluwer, Privacy Law in Marketing, 2009 WL 3619394 ¶ 15,020 (2014)
Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussion Between the European Commission and the United States Government*, DG MARKT Doc. 5092/98, WP 15 (Jan. 26, 1999)
Xiaoni Zhang et al., *A Cross-Cultural Analysis of Privacy Notices of the Global 2000*, 3 J. Info. Privacy & Security 18, 27 (2007)

CONTENTS

DATA PRIVACY AND INDIVIDUALISM: AN EXAMINATION OF THE TRANSATLANTIC PRIVACY DIVERGENCE

I. INTRODUCTION

In 1995, the European Union passed its Data Protection Directive.[1] The Directive confined the flow of consumer information to countries with "adequate" data privacy laws.[2] At the time, there was a good deal of uncertainty over the impact it would have on United States tech firms that offered services in the EU.[3] Until recently, the U.S.-EU Safe Harbor agreement has alleviated those concerns by allowing U.S. firms to certify compliance with a set of standards intended to enforce "adequate" data privacy protections for the purposes of the Directive.[4]

Now, however, EU politicians are beginning to question whether the Safe Harbor agreement actually provides adequate data privacy protections, once again leaving the future uncertain for U.S. tech firms in the European market.[5] With billions of dollars in liability or compliance costs at stake, the renewed debate is sure to cause firms considering investment in Europe to think twice about it.[6]

Meanwhile, the European Court of Justice ruled earlier this year that consumers may demand that search engine providers hide negative information about them from internet search

---

[1] Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 95/46/EC (Oct. 24, 1995) [hereinafter Data Protection Directive].
[2] *Id*.
[3] *See* U.S. Dep't of Commerce, *U.S.-EU Safe Harbor Framework*, Export.gov (last visited Nov. 15, 2014); Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussion Between the European Commission and the United States Government*, at 4, DG MARKT Doc. 5092/98, WP 15 (Jan. 26, 1999).
[4] U.S. Dep't of Commerce, *U.S.-EU Safe Harbor Guide to Certification*, Paper (June 16, 2013), *available at* http://export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_061613.pdf.
[5] *E.g*., Stephan Gardner, *EU Justice Nominee Notes Data Protection, U.S.-EU Safe Harbor at Nomination Hearing*, BLOOMBERG BNA (Oct. 6, 2014), *available at* http://www.bna.com/eu-justice-nominee-n17179895731/.
[6] *See, e.g.*, Olivia Solon, *Compliance with EU cookie law could cost the UK £10 billion*, WIRED UK (Apr. 24, 2012), *available at* http://www.wired.co.uk/news/archive/2012-04/24/eu-cookie-law-compliance-%C2%A310bn.

results.[7] Since then, Google has received a staggering 144,954 takedown requests, implicating 497,695 URLs.[8] Google employees must manually evaluate each request to determine whether the link qualifies for removal under the court's amorphous standard of "inadequate, irrelevant or no longer relevant, or excessive" information.[9] When consumers assert similar rights in US courts, however, they are routinely rebuffed.[10]

This paper explores these differing results in light of U.S. and EU cultures, positing a correlation between the relative importance that each jurisdiction places on individual autonomy and its conception of the state's role in data privacy regulation.

II. BACKGROUND

a. Background on U.S. and EU Privacy Law

For the purposes of this paper, there are two important dichotomies within legal conceptions of privacy. First, in both the U.S. and the EU, privacy has informational and decisional elements.[11] The informational dynamic refers to an individual's ability to control the things others know about her.[12] For example, the U.S. and European cultures tend to agree that things like health information and financial data are informational privacy concerns.[13] On the

---

[7] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos*, Case C-131/12 (Court of Justice of the European Union, May 13, 2014) [hereinafter *Google Spain*], *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131.

[8] Lance Whitney, *Google hit by more than 144,000 'right to be forgotten' requests*, CNET (Oct. 10, 2014), *available at* http://www.cnet.com/news/google-hit-by-more-than-144000-right-to-be-forgotten-requests/.

[9] *Google Spain*, C-131/12, Judgment at ¶ 92.

[10] *See, e.g.*, Zeran v. AOL, 129 F.3d 327 (4th Cir. 1997); Sidis v F-R Publishing Corporation 311 U.S. 711 (1940).

[11] *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2058 (2004) (discussing the differences between informational and decisional privacy). *Compare* Griswold v. Connecticut, 381 U.S. 479 (1965) (embracing the decisional privacy right to access contraceptives) *with* United States v. Jones, 132 S. Ct. 945 (2012) (recognizing an informational privacy right against prolonged GPS tracking).

[12] *Id.*

[13] *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (August 21, 1996) (codified in scattered sections of the U.S. Code) [hereinafter HIPPA]; Right to Financial Privacy Act of 1978, 12 U.S.C. 35 § 3401 *et seq.*; *see also* Virginia Boyd, *Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization*, 24 BERKELEY J. INT'L LAW. 939, 960 (2006) (comparing U.S. and EU financial privacy regulations) [hereinafter Boyd, *Financial Privacy*]; Data Protection Directive, *supra* note 1, at art. 1.

other hand, the decisional dynamic of privacy refers to the right to make inherently personal or intimate decisions.[14] Both cultures tend to acknowledge that things like parenting choices and sexual behavior are decisional privacy issues.[15] While the scope of the rights encompassed in either category varies greatly between the U.S. and EU, both systems recognize elements of each type of privacy. There exists excellent scholarship analyzing the comparative legal approaches in some facets of decisional privacy[16]; however, relatively little has been done to expand that analysis to informational privacy.

The second important dichotomy within legal conceptions of privacy is the distinction between government and private sector concerns. Government concerns include national security and local law enforcement entities. In this respect, U.S. and EU governments take somewhat similar approaches to privacy policy—and indeed, often even share information about their citizens.[17] On the other hand, each jurisdiction takes a unique path in addressing private sector concerns like consumer data collection, targeted marketing, and publication of intimate or damaging information.

---

[14] Schwartz, *Privacy, Property, and Personal Data*, *supra* note 11, at 2058.

[15] *See* Lawrence v. Texas 539 U.S. 558 (2003) (upholding decisional privacy in consensual sexual relations); Meyer v. Nebraska, 262 U.S. 390 (1923) (upholding decisional privacy in educating one's children); Modinos v. Cyprus, 7/1992/352/426 (European Court of Human Rights 1993) (upholding decisional privacy in consensual sexual relations under Article 8 of the European Convention on Human Rights), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57834; Wagner and J.M.W.L. v. Luxembourg 76240/01/458 (European Court of Human Rights 2007) (upholding decisional privacy right to adopt children without discrimination on marital status) *available at* http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=003-2054633-2174214.

[16] *See generally* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004) (applying an insightful autonomy-based analysis to European and U.S. privacy law with only tangential reference to data privacy) [hereinafter Whitman, *Two Western Cultures*].

[17] *See, e.g.*, Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEO. WASH. L. REV. 1162, 1177 (2011) (discussing "a number of (often classified) multilateral intelligence-sharing arrangements such as the relationship among the signals intelligence agencies of the United States, United Kingdom," and other countries).

The structure of U.S. and EU privacy frameworks are also different. The EU passed its seminal Data Protection Directive in 1995.[18] The Directive is specifically aimed at harmonizing the laws across its 28 member states.[19] It is an omnibus privacy regulation that applies to firms in all industries.[20]

By contrast, U.S. privacy regulations do not take the form of an omnibus statute.[21] U.S. privacy law consists of a patchwork of regulations, each covering a specific situation or industry that lawmakers have deemed high risks to privacy.[22] For example, the Video Privacy Protection Act ("VPPA"), enacted after the video rental history of unsuccessful Supreme Court nominee Robert Bork were publicized during his confirmation hearings,[23] regulates the circumstances in which a movie rental business may disclose the rental history of its customers.[24] To take a more well-known example, the Health Insurance Portability and Accountability Act ("HIPAA") requires that businesses dealing with "protected health information" protect the privacy of that data and obtain consent to its use.[25]

---

[18] *See* Data Protection Directive, *supra* note 1. The Directive expanded on a prior declaration; *see* Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS no. 108 (Jan. 28, 1981).
[19] WOLTERS KLUWER, PRIVACY LAW IN MARKETING, 2009 WL 3619394 ¶ 15,020 (2014) ("While EU directives are meant to have a harmonizing effect, in reality there are significant differences in member state transposition.").
[20] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW, 1109-1114 (4th ed. 2011) (overviewing the EU Data Protection Directive, and providing that "the Directive has encouraged the rise of omnibus legislation throughout the EU and most of the world.").
[21] Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013) (explaining that the U.S. "regulates information privacy on a sector-by-sector basis") [hereinafter Schwartz, *Privacy Collision*].
[22] Hogan Lovells, *EU and U.S. privacy proposals converge on principles, diverge on method*, GLOBAL MEDIA & COMMUNICATIONS QUARTERLY (Spring 2012), *available at* http://www.hoganlovells.com/files/Publication/7577188a-0174-4050-9db4-1b66747b423a/Presentation/PublicationAttachment/dba09642-5d75-44e0-ab18-1f8c6704398f/EU_and_US_privacy_proposals_converge_on_principles_diverge_on_method.pdf (describing variable U.S. privacy standards for different economic sectors).
[23] Andrea Peterson, *How a failed Supreme Court bid is still causing headaches for Hulu and Netflix*, WASHINGTON POST (Dec. 27, 2013), *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/27/how-a-failed-supreme-court-bid-is-still-causing-headaches-for-hulu-and-netflix/.
[24] *See* Video Privacy Protection Act, 18 U.S.C. § 2710.
[25] *See generally* HIPPA, *supra* note 13. *See also* U.S. Dep't of Health and Human Servs., *Summary of the HIPAA Security Rule*, HHS.GOV (last visited Nov. 15, 2014), http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html.

b. Background on the Individualism-Collectivism Cultural Framework

This paper draws heavily on the concepts of individualism and collectivism. Social scientist Geert Hofstede defines these terms in the following way:

> Individualism pertains to societies in which the ties between individuals are loose: everyone is expected to look after himself or herself and his or her immediate family. Collectivism as its opposite pertains to societies in which people from birth onwards are integrated into strong, cohesive ingroups, which throughout people's lifetime continue to protect them in exchange for unquestioning loyalty.[26]

This paper posits a correlation between a jurisdiction's privacy law and its social orientation toward collectivism or individualism. Specifically, this paper accepts that the U.S. tends to be more individualistic than Europe,[27] and suggests that certain differences between U.S. and EU privacy law may result from corresponding variations between the two jurisdictions' social orientations.

This paper identifies two salient applications of this theory. The first application deals with the fact that the U.S. is more likely than the EU to prefer minimally disruptive means of privacy regulation, consistent with the individualistic instinct to trust the citizen "to look after himself or herself."[28] The second application helps explain why the U.S. is more likely than the

---

[26] Ilhyung Lee, *The Law and Culture of the Apology in Korean Dispute Settlement (with Japan and the United States in Mind)*, 27 MICH. J. INT'L L. 1, 15 (2005) [hereinafter Lee, *Law and Culture*] (quoting GEERT HOFSTEDE, CULTURES AND ORGANIZATIONS, SOFTWARE OF THE MIND: INTERCULTURAL COOPERATION AND ITS IMPORTANCE FOR SURVIVAL 13-14 (1997) (hereinafter HOFSTEDE, CULTURES AND ORGANIZATIONS).

[27] *See* Pew Research Center, *The American-Western European Values Gap*, GLOBAL ATTITUDES PROJECT (Feb. 29, 2012), *available at* http://www.pewglobal.org/2011/11/17/the-american-western-european-values-gap/ ("As has long been the case . . . Americans are more individualistic . . . than are the publics of Britain, France, Germany and Spain."); *see also* HOFSTEDE, CULTURES AND ORGANIZATIONS, *supra* note 26 at 53 (indexing societal orientations toward individualism and finding that the U.S. scores substantially higher than most European countries).

[28] Research suggests that individualistic cultures exhibit more skepticism toward government regulation than collectivist ones, instead deferring to individual autonomy and market forces. *See* Lucian G. Conway et al., *Collectivism and Government-Initiated Restrictions: A Cross-Sectional and Longitudinal Analysis Across Nations and Within a Nation*, 37 J. CROSS-CULTURAL PSYCH. 20, 28-34 (2006) (finding strong correlation between collectivist cultural orientations and societal "tendency to restrict individual freedom while potentially preserving rights for the group."). That broad phenomenon seems to hold true in more specific inquiries as well, such as attitudes toward physician assisted suicide, *see* Markus Kemmelmeier et al., *Individualism and Authoritarianism Shape Attitudes Toward Physician-Assisted Suicide*, 29 J. APPLIED SOCIAL PSYCH. 2613 (1999); attitudes toward gun rights, *see* Katarzyna Celinska, *Individualism and Collectivism in America: The Case of Gun Ownership and Attitudes toward Gun Control*, 50 SOCIOLOGICAL PERSPECTIVES 229 (2007); and attitudes toward affirmative action,

EU to uphold speech rights when they conflict with privacy regulations, consistent with the notion that individualistic societies are "primarily motivated by their own preferences, needs, rights, and the contracts they have established with others."[29]

c. Review of the Literature on Privacy and National Cultures

Researchers have repeatedly documented cultural differences in attitudes toward information privacy. One of the earliest large-scale comparative studies was IBM's 1999 Multi-National Consumer Privacy Survey.[30] That survey confirmed that the U.S. differs from the United Kingdom and Germany in the extent to which internet users in each nation engage in privacy protective behaviors, including reading website privacy policies and declining to purchase products from sites with inadequate privacy protections.[31] Simultaneously, the IBM survey found that German and U.K. consumers were more confident in their governments' privacy regulatory regime than were U.S. consumers.[32]

While the IBM survey did not explicitly engage Hofstede's work, subsequent research has tied differing privacy attitudes to his cultural dimensions. For example, a Florida Atlantic University study applied Hofstede's indices to explain differences between U.S. and South Korean university students' use of privacy protective technologies, focusing primarily on

---

see Markus Kemmelmeier, *Individualism and Attitudes Toward Affirmative Action: Evidence From Priming Experiments*, 25 BASIC AND APPLIED SOCIAL PSYCH. 111 (2010). Other studies indicate that this pattern applies to at least some elements of consumer privacy regulation, *see* Charles R. Taylor et al., *Attitudes toward Direct Marketing and Its Regulation: A Comparison of the United States and Japan*, 19 J. PUB. POL. & MARKETING 228, 230, 234 (2000) (explaining that "it has been well documented that Japan is a more collectivist culture than the United States" and ultimately finding that U.S. respondents were significantly less likely to agree that "the government should exercise more control over both direct mail and telemarketing"); Geng Cui et al., *Consumers' Attitudes toward Marketing: A Cross-cultural Study of China and Canada*, 20 J. INT'L. CONSUMER MARKETING 81 (2008) (finding that "the Chinese are less likely to complain or engage in negative word-of-mouth, but they are more supportive of government actions and public resolution").

[29] Lee, *The Law and Culture*, *supra* note 26 at 15.

[30] Joy M. Sever et al., *IBM Multi-National Consumer Privacy Survey*, WHITE PAPER (Oct. 1999), *available at* http://web.archive.org/web/20060908210844/http://www.asc.upenn.edu/usr/ogandy/ibm_privacy_survey_oct991.pdf.

[31] *Id*. at 17.

[32] *Id*. at 18.

antispyware applications.[33] The researchers hypothesized that U.S. students were more likely to adopt antispyware technologies because, among other factors, U.S. individualistic tendencies would correlate with lower dependency on group norms in technology adoption, and higher rates of individualized privacy protective actions.[34] That study found that while students in both nations expressed an intent to protect their data from spyware, U.S. students were, in fact, substantially more likely to follow through by adopting antispyware technologies.[35]

Additional research confirms this analysis. One study examined the perceived value of corporate websites, and found that consumers in individualistic societies placed relatively greater importance on the privacy protection practices of the websites.[36] Another recent study found that subjects in individualistic nations were more likely to implement technological measures to guard access to their online identities.[37] Other studies have confirmed similar links between national culture and privacy attitudes.[38]

Finally, one study sought to examine the effects of individualism on overall level of information privacy concerns, as well as on the degree of national privacy regulations.[39] That study found that information privacy concerns remained largely static over the individualism-

[33] Tamara Dinev et al., *User Attitudes toward Protective Technologies*, 19 INFO. SYSTEMS J. 391 (2009).
[34] *Id*. at 394-96.
[35] *Id*. at 399-401.
[36] Jan-Benedict E.M. Steenkamp & Inge Geyskens, *How Country Characteristics Affect the Perceived Value of Websites*, 70 J. MARKETING 136 (2006).
[37] Princely Ifinedo, *The Effects of National Culture on the Assessment of Information Security Threats and Controls in the Financial Services Industry*, 12 INT'L J. ELECTRONIC BUS. MGMT. 82 (2014).
[38] *See id*. (*citing* Allen C. Johnston & Merrill Warkentin, *National Culture and Information Privacy: The Influential Effects of Individualism and Collectivism on Privacy Concerns and Organizational Commitment*, 1 INT'L FED. INFO. PROCESSING PAPER 88 (2009)); Tamara Dinev et al., *Privacy calculus model in e-commerce – a study of Italy and the United States*, 15 EUR. J. INFO. SYSTEMS 389 (2006).
[39] Sandra J. Milberg et al., *Values, Personal Information, and Regulatory Approaches*, 38 COMMS. OF THE ACM 65 (1995).

collectivism spectrum.[40] Nonetheless, it found that individualistic countries tended to enact less stringent forms of privacy regulation.[41]

III. ANALYSIS

a. The Individualism-Collectivism Framework Helps Explain the U.S.-EU Difference in Means of Privacy Regulation

In both the U.S. and the EU, privacy regulations typically codify various Fair Information Practice Principles ("FIPPs") into law.[42] FIPPs are expressions of the behavior expected from organizations that collect consumer data.[43] This section considers the following FIPPs in light of the individualism-collectivism framework: notice of collection; consent to collection; foreign transfer restrictions; and limitations on automated decisionmaking.[44] Under the principles of notice and consent, consumers are afforded a chance to understand the scope of information that a business intends to collect about them. Consumers may then either consent to the data collection or decline the proposed transaction. Foreign transfer restrictions are prohibitions against transferring data to third parties not subject to the laws of the jurisdiction in which the data was collected. Limitations on automated decisionmaking regulate the use of consumer information automatically to offer or deny a product, service, or other opportunity based on a consumer's information profile.

---

[40] *Id*. at 71.
[41] *Id*. at 72.
[42] *See* Schwartz, *Privacy Collision*, *supra* note 21 at 1969. Note that Professor Schwartz adopts the minority formulation of "Fair Information Practices" or "FIPs." *Id*.
[43] *Id*.
[44] *See id.*; *see also* U.S. Nat'l Inst. Science & Tech., *Fair Information Practice Principles (FIPPs)*, NIST.GOV (last visited Nov. 15, 2014), http://www.nist.gov/nstic/NSTIC-FIPPs.pdf; FTC, *Fair Information Practice Principles*, FTC.GOV (last visited Nov. 15, 2014), http://web.archive.org/web/20130303163422/http://www.ftc.gov/reports/privacy3/fairinfo.shtm (intriguingly, the FTC has scrubbed this document from its servers; however, it remains accessible via the preceding link to the Internet Archive's Wayback Machine); Robert Gellman, *Fair Information Practices: A Basic History*, BOBGELLMAN.COM (last visited Nov. 15, 2014), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

Some FIPPs, like notice and consent, find clear analogues in traditional doctrines of *laissez faire* private law, and thus appear to be relatively compatible with individualistic cultures.[45] For example, the notions of "offer" and "acceptance" in contract law incorporate the concepts of notice and consent.[46] An agreement imposes legal obligations only when it is not coerced—i.e., consensual—and only when it is not deceptive—i.e., adequate notice of the terms is available.[47] In this sense, notice and consent requirements treat consumer data like their property: the consumer owns her personal information in fee simple, and may choose to alienate certain sticks from the privacy bundle (her interests, location, age, contacts, etc.) in exchange for services or price reductions that are of greater value to her than retaining privacy in the data in question.[48]

Note, however, that notice and consent requirements do not *enhance* individualistic values relative to an unregulated market; consumers already have the right to refuse consent to data collection by declining to use the service that would otherwise collect it.[49] Nonetheless, state-enforced notice and consent requirements represent comparatively minor intrusions on individual autonomy because notice and consent typically exist even in the absence of a

[45] *See supra* note 28.
[46] *See, e.g.*, Randy E. Barnett, *A Consent Theory of Contract*, 86 COLUM. L. REV. 269, 271 (1986) ("Properly understood, contract law is that part of a system of entitlements that identifies those circumstances in which entitlements are validly transferred from person to person by their consent. Consent is the moral component that distinguishes valid from invalid transfers of alienable rights.").
[47] For competing perspectives on what constitutes notice and consent, *compare* Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997) *with* Specht v. Netscape Commc'ns Corp., 306 F.3d 17 (2d Cir. 2002). While Judges Easterbrook and Sotomayor differ in their conceptions of notice and consent, both agree that if notice and consent is lacking, no contract would exist. *Id*. There exists a related debate with respect to the 'consent' FIPP, with EU consent requirements typically demanding unambiguous affirmative assent, while U.S. consent requirements are generally satisfied by allowing the consumer a choice to opt out. *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1897 (2013).
[48] *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 142-43 (1999) (conceptualizing consumer data as property); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004) (discussing the benefits and difficulties associated with treating consumer data as property).
[49] This claim is distinct from an assertion that state-enforced notice and consent requirements do not increase overall consumer welfare, a proposition that is beyond the scope of this paper.

government requirement: notice of a service provider's ability to collect the data that a user submits to its website or application is a matter of common sense—and is often explicitly supplied in the form of terms of use.[50] Likewise, consent is manifested in the acceptance of those terms, or simply in the use of the service.[51]

The function of notice and consent requirements, then, is to transform the privacy tradeoff that is implicit in voluntary electronic transactions into a more discrete and explicit bargaining process. Notice and consent requirements, at least in their more modest iterations, appear to impose only minor restrictions on consumers' ability to "look out for [themselves]" and to guard their privacy through "the contracts they have established with others."[52] Therefore, an individualism-collectivism based analysis would predict that the U.S. privacy regulations, to the extent they exist, will rely more heavily on notice and consent than more disruptive FIPPs.

The legal consensus seems to support this prediction. In comparing U.S. and EU law, leading privacy scholar Professor Paul Schwartz has explained that the U.S. demonstrates relatively heightened reliance on notice and consent requirements, while the EU places "much less weight" on them, instead emphasizing other FIPPs.[53] Likewise, Marc Rotenberg, President

---

[50] *See, e.g.*, Mobile Marketing Association, *Mobile Marketing Association Releases Final Privacy Policy Guidelines for Mobile Apps*, Press Release (Jan. 25, 2012), *available at* http://mmaglobal.com/news/mobile-marketing-association-releases-final-privacy-policy-guidelines-mobile-apps (describing various attributes of notice that should be given by mobile app providers in their terms of use or privacy policies); Electronic Frontier Foundation, *Best Practices for Online Service Providers*, EFF.org (last visited Nov. 15, 2014), *available at* https://www.eff.org/files/eff-ospbp-whitepaper.pdf ("[A] privacy policy should accurately and completely disclose the privacy practices of the site."); FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, FTC.GOV (Mar. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[51] Boyd, *Financial Privacy*, *supra* note 13 at 980 (noting implicit consent through continued use).

[52] Ann Cavoukian et al., *The Unintended Consequences of Privacy Paternalism*, PRIVACY & INFORMATION COMM. WHITE PAPER 3-4 (Mar. 05, 2014), *available at* http://www.privacybydesign.ca/content/uploads/2014/03/pbd-privacy_paternalism.pdf (rejecting proposals to abandon notice and consent in favor of *ex post* government oversight as inherently paternalistic).

[53] Schwartz, *Privacy Collision*, *supra* note 21 at 1976.

of the Electronic Privacy Information Center has lamented the United States' "'notice and choice' formulation of privacy protection . . . that, embraced by the Federal Trade Commission, almost purposefully attempts to negate the range of rights that are to be found in the EU Data Directive."[54] Christopher Wolf, chair of the top Chambers-ranked privacy practice at Hogan Lovells, observed that "[a] major, if not defining characteristic of U.S. privacy law," is the FTC's targeted enforcement actions against firms that gave defective notice of privacy practices.[55] That disproportionate emphasis seems to be reflected in company practices. Researchers have found that notice is by far the most prominent FIPP manifested in U.S. firms' privacy policies,[56] and that U.S. firms focus substantially more on providing notice than do firms located in the United Kingdom.[57]

Other FIPPs, however, impose restrictions on the use of data that a firm has already collected.[58] These FIPPs generate ongoing obligations for businesses handling consumer data and "constrain[] the sovereignty of private business decision-making."[59] As a result, these *ex post* restrictions are generally more disruptive to the market and to individual autonomy than

---

[54] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 28 (2001) [hereinafter Rotenberg, *Fair Information Practices*].

[55] Christopher Wolf & Winston Maxwell, *So Close, Yet So Far Apart: The Eu and U.S. Visions of A New Privacy Framework*, 8 ABA ANTITRUST SYMP. 9 (Summer 2012) (explaining that "[h]istorically, the EU and United States have taken divergent approaches to implementing the FIPPs"); *see also* Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217, 1218 (2013) (contrasting the EU's Directive with the "'notice and choice' approach [that] gained credence in the United States").

[56] Alan Peslak, *Internet Privacy Policies: A Review and Survey of the Fortune 50*, 18 INFO. RESOURCES MGMT. J. 29 (2005).

[57] Xiaoni Zhang et al., *A Cross-Cultural Analysis of Privacy Notices of the Global 2000*, 3 J. INFO. PRIVACY & SECURITY 18, 27 (2007). The authors attribute the dominance of U.S. firms in the notice category to the structure of U.S. privacy law. *Id*. at 29 ("U.S. companies are expected to be more likely to comply with FTC principles . . . [t]herefore, it is natural for the U.S. to have the highest scores in the 'Notice' category.").

[58] Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 AM. BUS. L.J. 413, 456 (2013) [hereinafter King & Raja, *What Do They Really Know*] ("[C]ompanies that operate in the EU must comply with EU data protection law in terms of subsequent processing of personal data and sharing that data with other companies.").

[59] Gregory Shaffer, *Globalization and Social Protection: The Impact of Eu and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 16-20 (2000) [hereinafter *Shaffer, Globalization and Social Protection*] (discussing the costs of *ex post* requirements in terms of "personnel time, including time to review and revise all company practices, retain records, and respond to client information requests").

notice and consent requirements.[60] Consider the concept of limitations on automated decisionmaking. In practice, this means that automated determinations with significant impact on individuals—like qualification for a car loan—are lawful only if the firm making the decision informs the consumer that an automated decision will be made and provides access to the logic behind that automatic decision.[61] This requires the development of notice mechanisms, the tagging and tracking of data to ensure that renewed consent is obtained if the data is supplemented with information from other sources, and the implementation of a process for review of the factors contributing to the decision.[62]

Similarly, foreign transfer restrictions can prevent companies from realizing the full value of consumer data if that would require exporting the data to jurisdiction whose data protection laws the EU has not deemed adequate.[63] Foreign transfer restrictions provide an example of what Professor Anita Allen refers to as a "strongly coercive" privacy mandate because they "do not provide mechanisms of circumvention" [64] or other way to opt out of the restrictions. Foreign transfer restrictions effectively remove from individuals the choice to consent to transfers.

Unlike notice and consent requirements, these obligations do not permit consumers to alienate their rights to their personal information in fee simple. They raise transaction costs by

---

[60] *See supra* note 28 for a sample of the literature regarding the relationship between individualism and attitudes toward government intervention in the market.

[61] Data Protection Directive, *supra* note 1, art. 15(1) ("Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."); *id*. at Recital 41 ("[E]very data subject must also have the right to know the logic involved in the automatic processing of data concerning him").

[62] Andrej Savin, *Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks*, COPENHAGEN BUSINESS SCHOOL FACULTY REPOSITORY 3-7 (last visited Nov. 15, 2014), http://openarchive.cbs.dk/bitstream/handle/10398/8914/Savin.pdf (explaining that even explicit consent for automated processing may be insufficient if the information has subsequently changed hands or been supplemented with additional data).

[63] Matthias Bauer et al., *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, 3 EUR. CENT. INT'L POL. PAPER 2 (2014).

[64] Anita L. Allen, *Unpopular Privacy: The Case for Government Mandates*, 32 OKLA. CITY U. L. REV. 87, 99 (2007).

requiring specific consent for certain data uses, and nullify consumers' consent for others (such as data transfers to many foreign jurisdictions).[65] In discussing these *ex post* restrictions, Professor Shaffer has observed that "[t]he prices of goods and services on the EU market are, in principle, higher on average than they would be without the EU data privacy requirements."[66] As a result, these *ex post* requirements seem to be less compatible with individualistic values than notice and consent requirements. Accordingly, an individualism-collectivism based analysis would predict that the U.S. is less likely to implement these means of privacy protection than the EU.

The consensus seems to confirm that prediction; that is, privacy scholars appear to agree that limitations on automated decisionmaking and foreign transfer restrictions play large roles in EU protection, but are absent from U.S. law. Professor Schwartz has observed that "[s]ome FIPs are found exclusively in the EU regime. These EU elements are: . . . (6) enforcement mechanisms, including restrictions on data exports to countries that lack sufficient privacy protection; (7) limits on automated decisionmaking"[67] Other privacy law scholars have confirmed Schwartz' analysis with respect to automated decisionmaking limitations[68] and foreign transfer restrictions.[69]

---

[65] Data Protection Directive, *supra* note 1, at art. 25.
[66] Shaffer, *Globalization and Social Protection*, *supra* note 59, at 13 ("The European Union takes more of a legislative approach to data privacy protection than the United States, which relies more on private ordering through market processes.").
[67] Schwartz, *The EU-U.S. Privacy Collision*, *supra* note 21, at 1976.
[68] Graham Pearce & Nicholas Platten, *Orchestrating Transatlantic Approaches* to. *Personal Data Protection*: *A European. Perspective*, 22 FORDHAM INT'L L.J. 2024, 2040-41 (1999) ("[T]he EU directive seeks to ensure that individuals have the right to know the logic of any decisions about them taken by automatic means, the U.S. paper [setting forth U.S. privacy principles] makes no reference to such a provision."). Professor Daniel Solove recently coauthored an article with Professor Schwartz confirming that claim as well. Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877, 894 (2014) ("[T]he Directive provides protection against such decision making. . . . Here is an important distinction with U.S. information privacy law, which does not generally single out 'automated' decision making for special regulation.").
[69] King & Raja, *What Do They Really Know*, *supra* note 58, at 449 ("Unlike EU law, U.S. law does not restrict the transfer of consumers' personal data from the United States to other countries.").

Interestingly, in the case of foreign transfer restrictions, the individualist-collectivist divergence may be particularly stark because bans on transfers to other countries implicate both the individualistic aversion to government restrictions of autonomy and the collectivist tendency toward ingroup-outgroup distinctions. One study found that collectivist societies placed more importance on data transfers to foreign firms than transfers between domestic firms.[70] The authors concluded that "[a]lthough it may not be troubling to a collectivistic society to share personal data within their own group, it is not the same if it involves those outside the group."[71] The EU has also implemented other data privacy regulations that appear to reduce autonomy in response to collectivist concerns.[72] In sum, the means of privacy regulations used by the U.S. and EU seem to track the two jurisdictions' differences on the individualism-collectivism index.

In addition, both jurisdictions shared the same political impetus for the adoption of their privacy regimes. In 1981, the Organization for Economic Cooperation and Development ("OECD") promulgated a nonbinding report enumerating FIPPs that the OECD believed would promote economic development.[73] With its Directive, the EU sought to give binding force to these guidelines.[74] The Europeans had hoped that a singular, robust data protection regime could help close a dramatic gap between U.S. and EU data processing sectors, and spent several years

[70] Xiaoni Zhang et al., *A Cross-Cultural Analysis of Privacy Notices of the Global 2000*, *supra* note 70, at 18.
[71] *Id*. at 28.
[72] Anita L. Allen, *Unpopular Privacy: The Case for Government Mandates*, *supra* note 72, at 98 ("A U.S./European comparison helps to focus on the virtues of paternalism . . . Strikingly, the EU directive holds that some types of information are so sensitive that member states cannot collect it even with the consent of the individuals from whom it would be gathered. Now that's mandatory privacy, pure and simple. One can admire the 'inalienability' rule in EU information law, because it reflects appreciation of the dangers of data flow."). Note that the context of Professor Allen's observation indicates that the prohibition applies to both public and private actors in the "member states." *See also* Sarah Andrews, *Protecting Privacy Through Government Regulation*, 2 SEDONA CONF. J. 1, 7 (2001) (remarking that, relative to EU law, "[n]otably absent [the U.S.] definition [of the FIPPs] is any sort of 'collection limitation' principle prohibiting the collection of excessive data or its storage for a time longer than necessary").
[73] *See* OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, DOC. C 58 (Oct. 1, 1981).
[74] Fred H. Cate, *The Eu Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431 (1995).

debating how best to implement the OECD's recommendations.[75] The U.S. also endorsed this OECD report, and drew from it in forming its own early data privacy laws.[76] The EU's broader rules, however, in many ways seemed to reflect a uniquely European privacy paradigm. The automated decisionmaking limitations, for example, reflect a fear that a computerized decision "has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities."[77] The U.S. notice and consent regime, meanwhile, tends to maintain a more *laissez faire* quality.[78]

b. Limitations and Assumptions of the Preceding Means-of-Regulation Argument

To be sure, this analysis is hardly cut-and-dry. For one thing, there are often objectively greater protections for consent in EU law than in U.S. law. The EU Directive, for example, requires website proprietors to present their users with a conspicuous choice to opt out of tracking cookies;[79] the U.S., on the other hand, does not require consent or even notice of a website's cookie usage.[80] However, these instances of more stringent consent requirements in EU law are not necessarily inconsistent with the claim that consent plays a comparatively larger role in the U.S. data privacy framework than in that of the EU. Because consent requirements do

---

[75] *Id.*; Debra B. Rosler, *The European Union's Proposed Directive for the Legal Protection of Databases: A New Threat to the Free Flow of Information*, 10 HIGH TECH. L.J. 105, 109 (1995) ("Europe faces many obstacles to developing a strong, unified information technology system. Above all, the E.U. is hampered by linguistic fragmentation of its market and onerous labor laws. Europe holds a 30 percent share of the world's database production, but its industry maintains a much slower growth rate than that of the United States.").

[76] Schwartz, *The EU-U.S. Privacy Collision*, *supra* note 21, at 1970.

[77] European Commission, *Council Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data*, EXPLANATORY MEMORANDUM, COM (92) 422 final at 26.

[78] *See supra* notes 46-52 and accompanying text; *see also* Rotenberg, Fair Information Practices, *supra* note 54, at 26-28.

[79] European Commission, *Summary of Act: Data protection in the electronic communications sector*, EUROPA.EU (last visited Nov. 15, 2014) http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm; International Chamber of Commerce, *ICC UK Cookie Guide*, INTERNATIONAL-CHAMBER.CO.UK (Apr. 2012), http://www.international-chamber.co.uk/components/com_wordpress/wp/wp-content/uploads/2012/04/icc_uk_cookie_guide.pdf.

[80] At least, the U.S. federal government does not require cookie disclosures; some states do require it. *See, e.g.*, California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004).

not enhance autonomy, but merely are minimally intrusive on it, one would not expect to see an objectively higher incidence of consent requirements in the U.S.; one would expect only to see consent requirements emerge as one of the most important FIPPs in the U.S. regulations that do exist.

It is likewise admittedly the case that autonomy is, at best, only one of a network of complex and interrelated factors affecting privacy policy. For example, Professor James Whitman has argued that U.S. and European privacy law has fundamentally historical underpinnings, drawing on elements of phenomena ranging from feudal legal systems to dueling practices.[81] Whitman sought to dispel intuitionist approaches to privacy, which assume that there is a uniform slate of ideal privacy protections that may be derived from one's innate sense of what constitutes a privacy violation.[82] Instead, Whitman proposed that Americans and Europeans simply perceive privacy differently as a result of cultural programming.[83] Whitman argued that Europe, historically steeped in cultural notions of honor and personal reputation, has developed its privacy law around the core concept of dignity.[84] Whitman suggests that American culture, by contrast, does not share the European preoccupation with dignity, and instead fixates on the concept of liberty.[85] American privacy law, therefore, consists primarily of protections against the state rather than against private parties.[86]

Whitman's historical account doubtless supplies a plausible explanation for the differences in U.S. and European conceptions of privacy. Whitman's argument, however, does not seem to foreclose the possibility that the individualism-collectivism framework can help

[81] *See generally* Whitman, *Two Western Cultures*, *supra* note 16.
[82] *Id*. at 1154.
[83] *Id*.
[84] *Id*. at 1164.
[85] *Id*.
[86] *Id*.

explain differences in the U.S. and EU privacy regimes. In fact, it is possible that the historical cultural factors Whitman identifies—like European feudalism—inform modern European attitudes toward individualism and collectivism.[87] Moreover, even Whitman's liberty-dignity dichotomy seems to roughly track an individualism-collectivism framework. Individualistic societies tend to be more concerned with liberty-based considerations like personal autonomy, while collectivist societies are more likely to be concerned with dignity-based considerations like ingroup reputation.[88]

Another pertinent factor may well be the deep-rooted European mistrust toward large firms. That is, Europeans may be more likely than Americans to ascribe nefarious motives to corporate actors and harbor concerns that a market-based economy will lead to exploitation of consumers.[89] That attitude could result in a preference for regulatory frameworks that limit the set of agreements firms and consumers may enter to those deemed socially acceptable and non-exploitative. Nevertheless, a relatively greater preference for regulations in the marketplace appears to be the natural collectivist corollary of the individualist aversion to government

[87] Walter B. Kennedy, *Law and the Railroad Labor Problem*, 32 YALE L.J. 553, 559 (1923) ("American individualism is not our English or Scottish individualism *with its feudal or clannish restrictions of caste and class* . . . . It is very broad and deep, this American individualism, and has been the secret of American achievement from first to last, whether in the realms of war or peaceful progress.") (*quoting* Lt. Col. Chas. A. Repington, [*Untitled*], WASH. TIMES, (Nov. 19, 1922)) (emphases and ellipses in original); *see also* Avigail Eisenberg, *Individualism and Collectivism in Northern Politics*, 1 BRIT. COLUM. POL. STUDIES ASSOC. 6 (1995) (describing the effects of "the collectivist values of feudalism" on the development of the British political system).

[88] Recall that individualists "are primarily motivated by their own preferences, needs, rights, and the contracts they have established with others," while collectivists "see themselves as parts of one or more collectives (family, co-workers, tribe, nation) [and] are primarily motivated by the norms of, and duties imposed by, those collectives." Lee, *Law and Culture*, *supra* note 26 at 14-15.

[89] *See, e.g.*, Ron Shevlin, *In Banks We Mistrust*, AITE GROUP (Oct. 21, 2009) ("[D]espite the financial crisis in the United States, Americans still have a higher level of trust in their banks than British or French consumers have in theirs."), *available at* http://www.aitegroup.com/report/banks-we-mistrust-something-french-americans-and-british-agree-upon.

interference in the market.[90] Consequently, European skepticism of business seems to comport with, rather than undermine, application of the individualism-collectivism framework.

c. The Individualism-Collectivism Framework Helps Explain the U.S.-EU Difference on Conflicts Between Privacy and Speech

One may also apply an individualism-based explanation to U.S. and EU approaches to the intersection between privacy regulation and freedom of speech. This mode of analysis supplies a helpful perspective on privacy policy because the concept of freedom of speech is a largely a protection of individual autonomy.[91] To be sure, there exists in American literature a debate over the extent to which the First Amendment protects speech for individualist reasons like self-realization or for more collectivist purposes like personal dignity or social stability.[92] Nevertheless, most agree that individualistic justifications counsel in favor of more comprehensive speech protection, while collectivist justifications allow for speech restrictions.[93] Privacy regulation, on the other hand, often curtails individual autonomy to varying degrees.[94]

---

[90] *See supra* note 28 for a sample of the literature regarding the relationship between individualism and attitudes toward government intervention in the market.

[91] Fredrick Schauer, *The Exceptional First Amendment*, HARV. UNIV. FACULTY WORKING PAPER SERIES (February 2005), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=668543 ("Many of the controversies about freedom of speech present conflicts between liberty and equality, with the issues regarding hate speech and many forms of pornography among the most noteworthy. Moreover, these controversies between liberty and equality, as well as other conflicts between liberty and what might broadly be called 'civility,' also highlight a difference between, loosely and roughly, an individualist or libertarian view of the world, and, again loosely and roughly, a collective or communitarian view of the world. And to the extent that such contrasts reflect real differences, it would not be implausible to understand American free speech exceptionalism as a manifestation of the strong libertarian and individualistic aspects of American society itself.").

[92] *E.g.*, Calvin R. Massey, *Hate Speech, Cultural Diversity, and the Foundational Paradigms of Free Expression*, 40 UCLA L. REV. 103, 115 (1992) (recounting the contours and implications of competing First Amendment rationales).

[93] Guy E. Carmi, Di*gnity-the Enemy from Within: A Theoretical and Comparative Analysis of Human Dignity As A Free Speech Justification*, 9 U. PA. J. CONST. L. 957, 973 (2007) ("Most accounts of the autonomy defense are nonconsequentialist and therefore, according to Brison, aim to show 'why the right to free speech is immune to balancing.'") (*quoting* Susan J. Brison, *The Autonomy Defense of Free Speech*, 108 ETHICS 312, 339 (1998)).

[94] *See supra* notes 58-66 and accompanying text for a discussion of effects of privacy regulation on individual autonomy. *See also* Adam Thierer, *Is Privacy an Unalienable Right? The Problem with Privacy Paternalism*, TECHNOLOGY LIBERATION FRONT (Jan. 27, 2014), http://techliberation.com/2014/01/27/is-privacy-an-unalienable-right-the-problem-with-privacy-paternalism/; Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*,

Thus, one would expect an individualistic society like the U.S. would protect the free speech right at the expense of privacy regulations when the two are at odds with each other, while a more collectivist society would protect privacy regulations at the expense of free speech.

In fact, an examination of relevant U.S. and EU law comports with this paradigm. In the U.S., free speech is an enumerated constitutional right.[95] Over the years, the U.S. Supreme Court has taken that right seriously, invalidating legislation that would otherwise have protected personal privacy due to its speech-restrictive nature.[96] For example, in *Sorrell v. IMS Health*, a group of pharmaceutical manufacturers sought declaratory judgment against Vermont's Prescription Confidentiality Law on First Amendment grounds.[97] The law banned the practice, popular among pharmacists, of selling to pharmaceutical manufacturers statistics on the frequency with which individual doctors prescribed various drugs.[98] The pharmaceutical manufacturers would then use the information to tailor their marketing efforts to physicians.[99] The Prescription Confidentiality Law was a response to perceived violations of doctor privacy, but the effect was to silence pharmacists' speech, setting up a direct conflict between privacy regulation and free speech. The Court ruled in favor of the pharmaceutical manufacturer plaintiffs, thereby choosing to protect free speech.[100] The Court's reasoning is particularly instructive in this regard: having found that the regulation imposed a burden on free speech, the Court set out to determine whether the government's privacy rationale was sufficient to justify

126 HARV. L.REV. 1880, 1894-95 (2013) (discussing calls for privacy paternalism, their underlying assumptions about consumers, and their practical effects).
[95] U.S. CONST. amend. I.
[96] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of A Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000) (discussing the interaction between First Amendment jurisprudence and various information privacy regimes) [hereinafter Volokh, *Freedom of Speech*].
[97] Sorrell v. IMS Health Inc., 564 U.S. ___, 131 S. Ct. 2653 (2011).
[98] *Id.*
[99] *Id.*
[100] *Id.*

the infringement on free speech.[101] Noting that the statute was poorly tailored to advance a privacy interest, the Court held that in any event, the "unwanted pressure" doctors felt because their prescription decisions were being tracked was insufficient to justify a speech restriction.[102] The Court explained that "this asserted interest is contrary to basic First Amendment principles. Speech remains protected even when it may 'stir people to action,' 'move them to tears,' or 'inflict great pain.'[103]

Sorrell v. IMS Health is hardly unique among U.S. jurisprudence.[104] The Supreme Court has consistently invalidated privacy regulations as contrary to First Amendment free speech protections.[105] EU law, on the other hand, regularly makes precisely the opposite value judgment.[106] Article 10 of the European Convention on Human Rights, which purports to protect free speech, carefully circumscribes the right to cases that do not involve, *inter alia*, "the interests of national security . . . or . . . the authority and impartiality of the judiciary."[107] Indeed, many EU nations have *sub judice* rules that prohibit media discussion of cases currently under consideration.[108] These laws treat media publication of personal details about the plaintiff or defendant as contempt of court, and carry hefty penalties for violations.[109] Likewise, English

---

[101] *Id*. at 2667-2672.
[102] *Id*.
[103] *Id*. at 2670 (quoting Snyder v. Phelps, 562 U.S. ___, 131 S.Ct. 1207, 1220 (2011)). *Snyder* represents another case in which the Court protected free speech over privacy, holding that the First Amendment barred the plaintiff's infliction of emotional distress tort suit against a defendant who organized a vulgar protest at a funeral for the plaintiff's son.
[104] *See, e.g.*, Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975); Okla. Publishing Co. v. Okla. County District Court, 430 U.S. 308 (1977); Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979); Florida Star v. B. J. F., 491 U.S. 524 (1989).
[105] *Id*.
[106] *See* European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 10, ETS No. 5, 213 UNTS 221 (Nov. 4, 1950) [hereinafter European Convention on Human Rights].
[107] *Id*. at art. 10.
[108] See, e.g., McGarr Solicitors, *Sub Judice*, MCGARR BLOG (Jan. 24, 2007), *available at* http://www.mcgarrsolicitors.ie/2007/01/24/sub-judice/.
[109] *See id*.; *see also* Geoffrey Wheatcroft, *Privacy, Libel and the Case of Dominique Strauss-Kahn*, NAT'L INTEREST (May 19, 2011) ("Within living memory an editor of the Daily Mirror was sent to prison for transgressing the law on contempt when a case was still *sub judice*, and even now the most outrageous London cheap press would never publish the lurid detail the American tabs have bestowed on their readers about this particular 'perv perp' or 'frisky

plaintiffs may go to judges seeking injunctions against the publication of allegedly private details of their personal lives that, when granted, also prohibit any mention of the existence of an injunction.[110]

In its landmark decision *Von Hannover v. Germany*, the European Court of Human Rights ("ECHR") overruled the German high court's dismissal of a privacy tort case brought against two magazines for publishing paparazzi photos of the plaintiff, an adult daughter of a Monacan prince.[111] The photos were taken without the plaintiff's consent but otherwise legally, and depicted her engaged in various publicly-visible activities of day-to-day life, including eating at a restaurant, riding a horse, canoeing, and shopping. Like the U.S. Supreme Court in the above cases, the ECHR set out to balance the privacy interest against the concept of free speech.[112] There, however, the similarities end. The ECHR determined that "although freedom of expression also extends to the publication of photos, this is an area in which the protection of the rights and reputation of others takes on particular importance."[113] Consequently, the ECHR ruled that Germany had violated the plaintiff's privacy rights by failing to enforce her tort suit against the magazines.[114] That outcome—and even its "rights and reputation of others" language—presents a clear statement that, at least in ECHR, the collectivist notion that the government may suppress distasteful speech trumps the individualistic concept of free speech.

Frenchman.'"); Abdullah Bozkurt, *Intimidation toward press on 'sub judice' rule*, TODAY'S ZAMAN (Jan. 20, 2014), *available at* http://www.todayszaman.com/columnist/abdullah-bozkurt/intimidation-toward-press-on-sub-judice-rule_337090.html.

[110] *See* Wheatcroft, *Privacy*, *supra* n. 109 ("[I]n recent years English judges, ignoring what Americans would call First Amendment principles, have used the latter right [of respect for one's private life] to create a very wide-ranging concept of privacy. One judge in particular, Mr. Justice Eady, has almost single-handedly invented a new concept, the Orwellian 'super-injunction' which not only prohibits in advance any publication of unhappy details about the person seeking it but forbids any mention that such an injunction exists.").

[111] Von Hannover v. Germany, 2004 ECHR 294 (European Court of Human Rights, June 24, 2004), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-61853.

[112] *Id*. at para. 58.

[113] *Id*. at para 59.

[114] *Id*.

Other differences abound.[115] The EU Directive on Victims' Rights provides that "Member States shall ensure that competent authorities may take all lawful measures to prevent public dissemination of any information that could lead to the identification of a child victim."[116] By contrast, the U.S. Supreme Court, in *Cox Broadcasting v. Cohn*, held that the First Amendment barred a lawsuit brought against a news broadcaster by the father of a rape victim whose identity the broadcaster divulged, even though the victim was a minor.[117] The French prohibit the press from photographing handcuffed arrestees;[118] a U.S. court recently invalidated a law against surreptitiously photographing women from compromising angles in public.[119]

To recap, across numerous contexts in which information privacy regulations conflict with free speech rights, U.S. law consistently opts to protect speech, while European law often protects privacy regulations as acceptable limitations on speech rights. This result embodies the outcome one would expect if cultural attitudes toward autonomy substantially affect privacy policy because individualism facilitates near-absolutism on free speech issues, while collectivism implies that speech should give way where socially desirable ends like privacy regulations are at stake.

---

[115] Stephen Gardbaum, *The Myth and the Reality of American Constitutional Exceptionalism*, 107 MICH. L. REV. 391, 403-04 (2008) ("[I]n the conflict between the freedom of the press to report on criminal proceedings on the one hand, and both the right of the accused to a fair trial and the privacy interests of crime victims on the other, the United States stands alone in the degree to which it favors the former.").

[116] Directive establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision, 2012/29/EU, art. 25 (2012).

[117] Cox, *supra* note 104.

[118] Thomas Varela & David Gauthier-Villars, *France Urges Restraint From Media, Politicians*, WSJ (May 18, 2011), *available at* http://online.wsj.com/news/articles/SB10001424052748703421204576328982375553362.

[119] *Compare ex parte* Ronald Thompson, PD-1371-13 (Tex. Ct. Crim. App., Sept. 17, 2014) (holding that the First Amendment protects photographs of women in public when the photograph captures a perspective that is readily available for public observation) *with* Sinnott v. Carlow Nationalist (High Court of Ireland, 2008) (citation unavailable) (holding that defendant newspaper was liable for inadvertently publishing an in-game photograph of an English soccer player whose genitals were partially exposed), write up *available at* http://www.independent.ie/irish-news/player-gets-11000-for-offensive-photograph-26465705.html.

d. Limitations and Assumptions of the Preceding Privacy-vs-Free Speech Argument

In order to determine that free speech is an individual right, while privacy regulations are fundamentally intrusions on individual autonomy, this paper assumes (as do the First Amendment cases above) that personal information is *not* inherently the property of the consumer with whom it is associated.[120] That is, while one may protect her privacy by refraining from revealing information about herself—say, for example, her country of birth—if a firm deduces that information, perhaps by recognizing her distinctive accent, the firm has not 'stolen' anything from her.[121] She may hold the key to a plethora of information about herself, without which it would be exceedingly difficult to learn, but that information nevertheless does not belong to her in the sense that her car or her home belongs to her—and if another person learns that information, she has no right to demand that it be 'returned' to her.[122] This is typically not a controversial assumption, but it is also not necessarily self-evident.[123] While it may seem odd to say that one may own something that is perfectly nonexclusive—a "commodity" that everyone in the world could "possess" at the same time, like a phone number—in fact, intellectual property law provides exactly that.[124] Intellectual property law extends the notion of ownership beyond tangible things to information—to data.[125] If one conceptualizes consumer data as the intellectual property of the data subject, the above analysis becomes unworkable. Under such a

[120] *Cf*. Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996) (arguing that consumers have an intellectual property right in information about them).
[121] Volokh, *Free Speech*, *supra* note 96, at 1066-80 (discussing and ultimately rejecting any characterization of consumer information as consumer property).
[122] *See id*.
[123] *See, e.g.*, LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 142-43, *supra* note 48 (arguing for a property rights regime for consumer data).
[124] *See, e.g.*, Harper & Row Publishers, Inc. v. Nation Enterprises, 471 U.S. 539 (1985) (affirming a trial court's finding of liability against newspaper for publishing a portion of President Ford's memoirs, despite the overwhelming public interest in learning about the Watergate crisis elucidated therein).
[125] *See id*.; *see also* Am. Broad. Companies, Inc. v. Aereo, Inc., 134 S. Ct. 2498 (2014) (upholding copyright holder's intellectual property interest even in content that is broadcasted to the public for free over the airwaves).

framework, privacy laws would simply be another form of property protection legislation, like laws banning trespassing and theft.[126] Notions of individual autonomy, then, would demand that privacy laws be enforced—just as individual autonomy demands that laws against property crimes be enforced. Just as no one has a First Amendment right to trespass on private land or steal another's property, it would be impossible to argue from autonomy grounds that one has a First Amendment right to publish or sell information about another person.

In this way, the United States characterizes privacy differently for the purposes of First Amendment analysis than it does for the purposes of consumer protection as embodied in its notice and consent-based privacy regime. Recall from the discussion of U.S. FIPPs that notice and consent requirements treat consumer data similarly to property, and allow consumers to alienate that property by means similar to contract law. Although this is something of an inconsistency in the U.S. approach to privacy, it does not seem to undermine the suggestion that in both cases, individualistic considerations inform U.S. law, and can help explain differences between the U.S. and EU regimes to the extent such differences exist.

Additionally, one may note that the U.S. adopts a decidedly less individualistic posture toward privacy in the national security context.[127] For example, the U.S. federal government collects cell site location data from American citizens,[128] and supplies local police departments with tools to surveil U.S. citizens.[129] However, this paper does not seek to establish that the U.S.

---

[126] *See* Volokh, *Free Speech*, *supra* note 96, at 1063.
[127] *See, e.g.*, Robert Lemos, *FBI director to citizens: Let us spy on you*, ARS TECHNICA (Oct. 16, 2014), http://arstechnica.com/security/2014/10/fbi-director-to-citizens-let-us-spy-on-you/.
[128] Barton Gellman & Ashkan Soltani, *NSA tracking cellphone locations worldwide, Snowden documents show*, WASHINGTON POST (Dec. 04, 2013), *available at* http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.
[129] Megan Geuss, *Cops hid use of phone tracking tech in court documents at feds' request*, ARS TECHNICA (June 20, 2014), *available at* http://arstechnica.com/tech-policy/2014/06/cops-hid-use-of-phone-tracking-tech-in-court-documents-at-feds-request/.

is a consistently individualistic society; only that it is more so than its counterparts in the EU on privacy issues. On that inquiry, it seems that EU governments are hardly any more individualistic in their national security policy. Like the U.S., the UK's GCHQ has long sought to realize a "full take" approach to its citizens' private data.[130] Whistleblower Edward Snowden has alleged that GCHQ has a worse privacy record even than the NSA.[131] Ultimately, the U.S. approach to privacy in the national security setting does not necessarily seem to undermine the proposition that its private sector privacy policy largely reflects cultural tendencies toward individualism.

IV. CONCLUSION

In conclusion, the individualism-collectivism framework seems to provide a useful tool in evaluating U.S. and EU differences in the selection and application of FIPPs. Individualistic cultures, like the U.S., exhibit tendencies toward means of regulation that leave the market minimally disturbed, while collectivist cultures tend to exhibit more willingness to implement disruptive policies. That phenomenon can help explain the U.S. preference for notice and consent-based regulations and the EU's comparatively greater preference for *ex post* regulations of data collection.

Moreover, differences between U.S. and EU approaches to privacy and free speech conflicts are also susceptible to individualism-collectivism based analyses. Individualistic cultures tend to uphold free speech when it conflicts with privacy regulations, while more collectivist cultures are more willing to uphold privacy regulations at the expense of speech

[130] Der Spiegel, *Edward Snowden Interview: The NSA and Its Willing Helpers*, DER SPIEGEL (July 08, 2013), *available at* http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html.
[131] Russia Today, *'Test it on Brits:' Snowden says GCHQ even worse than NSA,* RT (July 20, 2014), *available at* http://rt.com/uk/174172-british-intelligence-lacks-oversight/.

rights. These tendencies likely contribute to the U.S.' well-documented preference for free speech over privacy rights in a variety of contexts, which contrasts with the EU's privacy preference. This paper accepts that a variety of cultural factors influence privacy policy. Nevertheless, at least in the case of U.S. and EU, policy differences seem to closely track the individualism-collectivism framework.

On my honor, I submit this work in good faith and pledge that I have neither given nor received improper aid in its completion.

/s/ Tony Glosson