The Transparent Citizen

*Joel R. Reidenberg**

This Article shows that the transparency of personal information online through ubiquitous data collection and surveillance challenges the rule of law both domestically and internationally. The Article makes three arguments. First, the transparency created by individuals' interactions online erodes the boundary between public and private information and creates a "transparent citizen." Second, the transparent citizen phenomenon undermines the state's faithfulness to the ideals of the rule of law and to citizens' respect for the rule of law. Transparency enables government to collect and use personal information from the private sector in ways that circumvent traditional political and legal checks and balances. Transparency encourages the development of anonymity tools that empower wrongdoers to evade legal responsibility and the rule of law. And, transparency puts national security, public safety, and legal institutions at risk in ways that will jeopardize and corrode the public's faith in the rule of law. Third and lastly, transparency challenges international norms and data flows. National data privacy law is anchored in local constitutional culture and the transparency of personal information across borders creates deep-seated political instability that will only be resolved through political treaties.

 A.B. Dartmouth; J.D., Columbia; Ph.D, Universite de Paris-Sorbonne. Stanley D. and Nikki Waxberg Professor of Law and Founding Director, Center on Law and Information Policy, Fordham University School of Law. I am indebted to Dan Solove for a discussion a number of years ago that inspired this Article and for the *Loyola University of Chicago Law Journal* for giving me the opportunity to present this work at the symposium. Work on this Article was supported by a faculty fellowship and summer research grant from Fordham University. Many thanks for helping me refine these thoughts over a number of years go to workshop participants at the Nobel Prize Week Public Service Summit, the Fordham Faculty Workshop, the Harvard Berkman Center Law Lab, the NYU Information Technology & Society Colloquium, the University of Pennsylvania CTIC Faculty Workshop, the Boalt Hall-GWU Privacy Law Scholars Conference, and especially Steve Bellovin, Danielle Citron, John Clippinger, Julie Cohen, Devan Desai, Ed Felten, Urs Gasser, Rebecca Hulse, Alexandra Lahav, Andrea Matwyshyn, Dierdre Mulligan, Helen Nissenbaum, John Palfrey, Paul Schwartz, Christopher Yoo, Ian Weinstein and Benjamin Zipursky. I would also like to thank Katherine Lenahan for providing excellent research assistance and Yehuda Hatsvi for finding several key quotes. Any errors and omissions remain the sole responsibility of the author.

Every single datum about my life is private? That's silly.[1]
- Justice Antonin Scalia

Privacy has long existed as a key value in western civilizations. As early as the Bible, history records efforts to protect privacy and prevent the transparency of private activities. In the Book of Numbers, during the exodus from Egypt the tribes of Israel are commanded to camp in the desert by family and Balaam says, "how goodly are thy tents o Jacob, thy dwellings o Israel."[2] Ancient biblical commentaries interpreted this passage to forbid dwelling windows or doors from opening directly opposite a neighbor's window or door and thus assure the privacy of the home.[3] Confidentiality was also highly valued. The Book of Proverbs says: "[H]e who goes about as a talebearer reveals

1. Noam Cohen, *Link by Link: Fordham Law Students Teach Scalia About Privacy and the Web*, N.Y. TIMES, May 17, 2009, at B3.

2. *Numbers* 24:2. In Numbers 24:32, the Bible even says "and so did they journey, each man with his family according to his father's house."

3. *Mishnah Bava Batra* 3:7.

secrets; but he who is trustworthy in spirit keeps a thing hidden."[4] The privacy of communications was also assured with penalties of excommunication from the community.[5]

In our modern times, the distinction between public and private information is similarly critical for a well-functioning democracy and is accorded protection in constitutional instruments.[6] Privacy enables citizens to engage in the deliberative process of democracy—by giving them the space to form thoughts and to interact socially and politically with others.[7] Indeed, the French Constitution[8] endorses the celebrated Declaration of the Rights of Man which enshrines that "the freedom to communicate thoughts and opinions is one of the most precious rights of man: any citizen can thus speak, write and publish freely."[9] More than two hundred years later, the United States Supreme Court in *McIntyre v. Ohio Elections Commission* was emphatic when it said, "under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority."[10]

In this age of blogs, Twitter, Flickr, Instagram, online search engines, social networking sites, webcams, and e-government, our private selves and our informational identity are, however, often on public display. In many ways, we face the same ancient issue, except now it is on steroids with cloud computing. Technology has truly enabled the creation of the "transparent citizen." While Justice Scalia is surely correct that information is often not private as a legal matter, his assertion that information privacy is "silly"[11] illustrates that in a democratic society

---

4. *Proverbs* 11:13.

5. *See* Nahum Rakover, *The Protection of Privacy in Jewish Law*, 5 ISR. Y.B. ON HUM. RTS. 169, 172 (1975).

6. For example, the U.S. Constitution through the Fourth Amendment enshrines the seclusion of a private zone against state interference. U.S. CONST., amend. IV. The Fifth Amendment assures autonomy for individuals with respect to disclosure of information to the state. *Id*. amend. V. The European Convention on Human Rights and Fundamental Freedoms explicitly establishes a "right to private and family life." Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 (as amended by Protocols No. 11 and No. 14), http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm.

7. *See* NEIL RICHARDS, INTELLECTUAL PRIVACY (2015); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

8. 1958 CONST. pmbl. (Fr.)

9. DECLARATION OF THE RIGHTS OF MAN AND OF THE CITIZEN art. XI (1789) (Fr.) ("La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme: tout Citoyen peut donc parler, écrire, imprimer librement . . . .").

10. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).

11. Cohen, *supra* note 1.

the governance dimension of the blending of publicly available and private information is poorly understood. Indeed, as it turned out, Justice Scalia did in fact believe that every datum in his life should be private.[12]

This Article seeks to show that the transparency of personal information in the network ecosystem through ubiquitous data collection and ambient surveillance creates a subtle, but fundamental challenge to governance through the rule of law both domestically and internationally.[13] As Lon Fuller articulated in his widely recognized principles for the rule of law, law must exist and be obeyed by all, including government.[14] The transparent citizen undermines the fulfillment of this basic precept of the rule of law. This challenge is international in scope and global information instability will be inevitable without an international political solution.

The Article makes three arguments. In Part I, the Article maps out the erosion of the border between public and private information in the network ecosystem on the Internet and the resulting "transparent citizen." Part II then argues that the transparency of personal information in the network ecosystem challenges democracy's principle of the rule of law. Part III shows that the challenge is international in scope and concludes by showing that global instability will be inevitable without an international political solution.

I. FROM TRANSPARENT PERSONAL INFORMATION TO THE TRANSPARENT CITIZEN

Data collection, storage, and processing are ubiquitous in the networked ecosystem. From grocery store purchases to telephone calls, client information is collected and stored for aggregation and networked data mining.[15] The ubiquity and ambient level of surveillance emerges from a variety of factors: network functionality, government functions,

12. *Id.*

13. This perspective situates privacy in the power struggle between democratic rule of law and network rule of technology. Elsewhere I have elaborated on this profound struggle in other network contexts. *See, e.g.*, Joel R. Reidenberg, *Baker Botts Lecture: The Rule of Intellectual Property in the Network Economy*, 44 HOUS. L. REV. 1073 (2007); Joel R. Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951 (2005); Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS J. 261 (2002).

14. LON L. FULLER, THE MORALITY OF LAW 39 (rev. ed. 1969) (advocating that a legal system will be a failure if there is "a failure to achieve rules at all . . . [and if there is] a failure of congruence between the rules as announced and their actual administration").

15. Ira Rubinstein, Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technical Approaches*, 75 U. CHI. L. REV. 261 (2008).

commercial goals, security, social media, and the impracticality of obscurity.

A. Network Functionality

The provision of networked services creates clickstreams that generate vast quantities of data about individuals.[16] Tracking information is necessary to route communications. For example, cell phones would not function without the geolocation of subscribers at all times. Cloud computing—the latest computing development that embeds data storage on network servers permitting access from any device connected to the Internet—necessitates robust information tracing. Internet communications require the tracing of transmission origin and end points to route traffic. Radio frequency identification ("RFID") chips are now implanted in passports to store personal information and facilitate border clearance procedures.[17]

B. Government Functions

The growth of open government and government benefits programs generates vast data collection needs.[18] Property tax rolls, public licenses such as driver's licenses, car and boat registrations, attorney registries, and sex offender registries, and other lists fuel the states' repositories of data. While much of this data has historically been available to the public through freedom of information statutes, government agencies are now making this data available online, thus increasingly disseminating the details of citizens' lives ranging from the value and floor plans of their homes,[19] to their political contributions,[20] to professional licenses,[21] to their parking tickets,[22] and even to their

16. *See, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004).

17. *See Passport Card*, U.S. DEP'T STATE, http://travel.state.gov/content/passports/en/passports/information/card.html (last visited Nov. 18, 2015).

18. *See* SOLOVE, *supra* note 16; Jack Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008).

19. *See, e.g.*, DARIEN, CT: ASSESSOR DATABASE, http://darien.ias-clt.com/parcel.list.php [https://web.archive.org/web/20120424132804/http://darien.ias-clt.com/parcel.list.php?] (last visited Nov. 18, 2015) (searchable database accessing public records of real estate transactions, which includes floor plans); *Property Search*, COOK COUNTY ASSESSOR'S OFF., http://www.cookcountyassessor.com/Property_Search/Property_Search.aspx (searchable database by address, neighborhood, or specific property identifier) (last visited Nov. 18, 2015).

20. *See, e.g.*, *Donor Lookup: Find Individual and Soft Money Contributors*, CTR. FOR RESPONSIVE POL., http://www.opensecrets.org/indivs/index.php (searchable database obtained from public filings required by election laws) (last visited Nov. 18, 2015).

21. *See, e.g.*, *eCourt Attorney Search*, N.Y. ST. UNIFIED CT. SYS., https://iapps.courts.state.

sex offender status.[23] Other government-collected data may not be released publicly at the moment, but future dissemination remains an open question. For example, many states collect and retain DNA samples from newborn babies without parental knowledge or consent.[24] The release of this data in the years to come—with varied justifications such as genetic studies—while speculative, is likely.

Legal mandates also compel the private sector to gather data about their clients. For example, U.S. financial institutions must help law enforcement agencies detect and prevent financial crimes.[25] Anti-money laundering regulations typically require that banks "know their customers" and mandate the gathering of client's demographic and identifying information.[26]

C. Commercial Pressures

In addition to network functionality and government programs, commercial pressures exponentially increase the need for and the gathering of personal information. Product personalization and one-to-one sales and marketing require detailed customer information or profiles. The latest trend in marketing is behavioral advertising that seeks to target product solicitations to individuals based on their actual Internet activities.[27] The targeting models rely on data mining from large data sets or "warehouses" of online behavior such as website

---

ny.us/attorney/AttorneySearch (searchable database of attorneys admitted to N.Y. state courts) (last visited Nov. 18, 2015).

22. *See, e.g.*, *NYCServ eService Center*, NYC, http://nycserv.nyc.gov/NYCServWeb/NYCSERVMain (searchable database of parking tickets, red light violations, water charges, health code violations, and consumer affairs violations) (last visited Nov. 18, 2015).

23. *See, e.g.*, *N.J. Sex Offender Internet Registry*, N.J. ST. POLICE, http://www.njsp.org/sex-offender-registry/index.shtml (searchable database of sex offenders registered in New Jersey) (last visited Nov. 18, 2015); Megan's Law Website, PA. ST. POLICE, http://www.pameganslaw.state.pa.us/ (searchable database of sex offenders) (last visited Nov. 18, 2015).

24. *See* Elizabeth Cohen, *The Government Has Your Baby's DNA*, CNN (Feb. 4, 2010), http://www.cnn.com/2010/HEALTH/02/04/baby.dna.government/index.html?hpt=C1.

25. *See Bank Secrecy Act*, U.S. DEP'T TREASURY CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/statutes_regs/bsa/.

26. *See* Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified in part at 31 U.S.C. §§ 5311–5332 (2012)). The Customer Identification Program ("CIP") implementing the Bank Secrecy Act requires banks to perform "[i]dentity verification procedures" that collect sufficient personal information about the bank's customers in order to enable the bank "to form a reasonable belief that it knows the true identity of each customer." 31 C.F.R. § 1020.220(a)(2) (2015).

27. *See About Google Ads*, GOOGLE, http://support.google.com/ads/answer/1634057?hl=en (last visited Nov. 18, 2012) ("You may see text ads on Google Search results pages and other Google products such as Google Maps. The ads you see may be based on what you searched for, your location, and the time of day.").

browsing and e-commerce transactions in combination with offline behavior.[28] As an early example, this was one of the motivations behind DoubleClick's acquisition of Abacus,[29] and then Google's subsequent acquisition of DoubleClick.[30] Tracking files and other surveillance technology are often installed automatically on a computer whenever its user visits a website.[31] In addition to gathering a user's search history, such technology can assess a user's location and personal information to target ads to that user more effectively.[32]

Back office functions further expand data collection. RFID chips are increasingly used to track store inventory. Alien Technologies, for example, had a joint venture with Lacoste, Calvin Klein, and Burberry to embed RFID chips in clothing.[33] This also means that RFID readers can monitor where people wear their Calvins. Similarly, Walmart embarked on a project to embed RFID tags so that the company would be able to track jeans and underwear.[34]

Commercial pressure then also creates a significant market for the dissemination of personal information. Companies sell information, whether through advertising or subscription, that discloses significant personal information.[35] At the same time, companies sell information that facilitates tracking individuals. For example, Google Earth reveals

---

28. *See Behavioral Targeting Solutions*, MICROSOFT, http://advertising.microsoft.com/en/behavioral-targeting (last visited Nov. 18, 2015) ("We use data from keyword searches and site visits to place users into dozens of valuable consumer segments most likely to be receptive to specific messages.").

29. *See* Courtney Macavinta, *Privacy Advocates Rally Against DoubleClick-Abacus Merger*, CNET NEWS (Jan. 2, 2002, 4:43 PM), http://news.cnet.com/2100-1023-233413.html.

30. Catherine Holahan, *Google's DoubleClick Strategic Move*, BLOOMBERG: BUS. (Apr. 14, 2007), http://www.bloomberg.com/bw/stories/2007-04-14/googles-doubleclick-strategic-movebusinessweek-business-news-stock-market-and-financial-advice; *see also* Jessica E. Vascellaro, *Google Agonizes on Privacy as Ad World Vaults Ahead*, WALL ST. J., Aug. 10, 2010, at A1 (chronicling Google's initial hesitancy to buy DoubleClick and eventual decision to sell targeted ads).

31. *See* Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 30, 2010, at W1.

32. *See id.*

33. *See* Press Release, Alien Technology Secures Fifth RFID Retailing Installation in Europe with Lacoste, Calvin Klein and Burberry (Feb. 16, 2009), www.alientechnology.com/newsevents/2009/press021609.php [https://web.archive.org/web/20120302030248/http://www.alientechnology.com/newsevents/2009/press021609.php].

34. Miguel Bustillo, *Wal-Mart Radio Tags to Track Clothing*, WALL ST. J., July 23, 2010, at A1.

35. Acxiom, for example, is one of the nation's largest sellers of personal information and, for a fee, will sell data on ethnic assimilation, age, wealth, and much more. *See* Consumer Data Products Catalog, ACXIOM, https://www.hashdoc.com/documents/8135/data-products-catalog (last visited Nov. 18, 2015).

street and home images.[36] These data sets can be overlaid to show, for example, the home locations and images of wanted criminals or hounded celebrities.

D. Security

Cybersecurity, physical security, and homeland security imperatives likewise create great pressures for surveillance and the tracking of online activities as well as data mining programs.[37] In the case of cybersecurity, network monitoring and traceability are essential to deter attacks. This necessitates what in 1988 Roger Clarke presciently termed "dataveillance."[38] Likewise, physical security concerns pressure organizations to deploy surveillance camera networks and monitors. Homeland security programs, in their efforts to deter attack, focus on profiling potential attackers through large-scale data collection and analysis.[39]

E. Social Media

Concomitant with the trend for business and government to collect and process more personal information online, social networking increases the disclosure and dissemination of personal information. Internet users independently reveal some of the most intimate details of their lives on blogs and websites. Facebook users routinely post information about their private lives—relationship status, religious affiliation, and latest party escapades.[40] Tweeters on Twitter record their real-time movements and thoughts for the world to see.[41] Friends

---

36. *See* GOOGLE MAPS, http://maps.google.com (last visited Nov. 18, 2015) (providing the "streetview" function, which allows users to see images of particular streets, and the "satellite" function, which allows users to view satellite images of streets and specific addresses).

37. *See, e.g.*, Patricia Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137 (2008); Christopher Slobogin, *Government Dragnets*, 73 L. & CONTEMP. PROBS. 107 (Summer 2010).

38. Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498 (1988).

39. *See generally* JEFFREY W. SEIFERT, CONG. RESEARCH SERV., RL 31798, DATA MINING AND HOMELAND SECURITY: AN OVERVIEW (2007), http://www.fas.org/sgp/crs/intel/RL31798.pdf (explaining data mining and its use and limitations in the Department of Homeland Security's counterterrorism measures).

40. *See* Spanierman v. Hughes, 579 F. Supp. 2d 292 (D. Conn. 2008); Snyder v. Millersville Univ., No. 07-1660, 2008 WL 5093140 (E.D. Pa. Dec. 3, 2008); Ian Shapira, *When Young Teachers Go Wild on the Web: Public Profiles Raise Questions of Propriety and Privacy*, WASH. POST, Apr. 28, 2009, at B3.

41. TWITTER, http://www.twitter.com/about (last visited Nov. 18, 2015). Twitter enables users to post 140 character "tweets" or messages to computers and cell phones via instant messaging, web posting, and texting. Registration is free and anyone can sign up to receive "tweets" from any user. *See, e.g.*, Mark Glaser, *NYU Professor Stifles Blogging, Twittering by*

and neighbors disclose information and the information of others when they post material on the web such as photographs or captured images from webcams.[42]

Yet, despite an individual's public dissemination of his or her personal information, there remains a sense that these disclosures exist for limited purposes. At the same time Internet users bare their souls online, they react harshly and negatively to the unexpected viewing of their personal information. Facebook faced vociferous criticism and lawsuits when it launched Beacon, a technology that telegraphed Facebook user's personal information and web actions to third parties.[43]

F. Loss of Practical Obscurity

The convergence of these factors leads to the loss of "practical obscurity" and an important expansion of the scope of personal data in the public sphere. Practical obscurity was a protection effectively afforded by the difficulty of access to information that was nonetheless formally in the public domain. For example, property records are quintessential public records. In the past, information might have been available on a homeowner's mortgage, but the voyeuristic neighbor had to go to the county recorder of deeds to find the original record among musty old property records. This practical difficulty made the "public information" generally obscure from prying eyes. However, now these records are made public online and search engines make these vast quantities of data readily available for all to see with only a few clicks of a keyboard.[44] In a famous pre-Internet case, *Department of Justice v. Reporters Committee for a Free Press*, the Supreme Court held that rap sheets were not public information for purposes of the Freedom of Information Act.[45] The Court recognized that "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single

---

Journalism Student, PBS MEDIASHIFT (Sept. 17, 2008), http://www.pbs.org/mediashift/2008/09/nyu-professor-stifles-blogging-twittering-by-journalism-student261.html.

42. *See, e.g.*, Jean v. Mass. State Police, 492 F.3d 24, 26 (1st Cir. 2007) (holding that webcam video taken illegally of a warrantless police search could be lawfully posted on the Internet).

43. Caroline McCarthy, *Facebook Beacon Has Poked Its Last*, CNET (Sept. 18, 2009, Sept. 19, 2009), http://news.cnet.com/8301-13577_3-10357107-36.html.

44. As an example, the execution of a few simple searches with well-chosen search terms on Google can often unveil a person's home address, telephone number, family members, mother's maiden name, level of political activity, hobbies, and photographs, to name just a few categories of available information. *See* Cohen, *supra* note 1.

45. U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749 (1989).

clearinghouse of information."[46]

This vast difference stems from the repurposing of personal information that arises with digitalization and compilations. In other words, data that is collected for one purpose in a particular context takes on a different character when processed or used outside that original context.[47] In effect, Justice Scalia, in joining the majority in *Reporter's Committee*, foreshadowed the transparency and loss of practical obscurity that arises with data mining on the Internet.

The loss of practical obscurity is often a poorly understood phenomenon. Typically, the scope of transparency of personal information and the ease of repurposing are a surprise to data subjects and the public at large. Even Justice Scalia, who anticipated the issue early on, did not recognize the profound implications. In January 2009, he gave a speech in New York and was quoted as saying that to treat much of the information on the web as private was "silly" and that he did not care whether people knew what groceries he bought.[48] As it turned out, Justice Scalia cared very much and did not think it was "silly." We learned this from Justice Scalia's intemperate response to a class exercise in an Information Privacy Law course that I taught at Fordham.[49]

As part of my Information Privacy Law course at Fordham, the class undertook a research exercise to explore the origins and scope of privacy law, the ways technology can both invade and protect personal information, and the relationship between law and those technologies.[50] The exercise had as an important aim: to illustrate the transparency and

---

46. *See id.* 764.

47. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 74 GEO. WASH. L. REV. 119 (2004). This re-purposing is also known as "secondary use" and is treated as an improper information practice without the data subject's consent. Org. for Econ. Cooperative & Dev. [OECD], *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 23, 1980) (revised 2013) [hereinafter OECD, *Guidelines*], http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; Council Directive 95/46, art. 25, 1995 O.J. (L 281) (EC). The concept is enshrined in various US statutes and regulations. *See, e.g.*, Fair Credit Reporting Act of 1968, 15 U.S.C. § 1681–1681x (2012)""; Cable Communications Policy Act of 1984, 47 U.S.C. § 521-573 (2012); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232(g) (2012).

48. *See* Jennifer Peltz, *Scalia Speaks on Digital Privacy at NYC Conference*, NEWSDAY (Jan. 28, 2009), http://www.lawjournalbuffalo.com/news/article/current/2009/02/02/100308/scaliaspeaks-on-digital-era-privacy-at-nyc-conference.

49. Cohen, *supra* note 1.

50. *See* Daniel Solove, *Justice Scalia's Dossier: Joel Reidenberg Responds*, CONCURRING OPINION (May 1, 2009), http://www.concurringopinions.com/archives/2009/05/justice_scalias_3.html (last visited Nov. 18, 2015).

secondary use associated with readily available information on the Internet. The exercise was designed to provide a first-hand experience for class discussion of the issues of contextual use, social norms, and the scope of legal protection. The class focused particular attention on the boundary between public and private information and the loss of practical obscurity. For the exercise several years ago, I framed the research as a challenge to the class to find a specific piece of esoteric information about me. Over the course of the semester, students posted links to web pages containing information about my family and me and through data mining analysis students were able to generate the target information. The class was surprised at how much information could be found readily.

The following year, the course syllabus focused greater attention on the blurring of public and private information, so the class exercise was framed to find information about a public figure. During a class discussion early in the semester of Justice Scalia's quotes about the silliness of privacy in his New York speech, the issues he raised about transparency made him a logical choice for the class research on a public figure. Like the previous year, class members posted publicly available information related to Justice Scalia to a password-protected discussion board. This in turn led to information about his family. To enhance a class review discussion on the issues of aggregation and secondary use, the loss of anonymity, and legal responses, one of the students prepared a fifteen-page compilation of the information in an organized dossier format. The class was shocked by the results—the extensive dossier on an individual and members of his family were all available from publicly accessible sources on the Internet. This was precisely the teachable point and it was not lost on Justice Scalia. Indeed to emphasize the value of the exercise as a pedagogical tool, the class dossier has remained a confidential, course document. None of Justice Scalia's personal information was ever published or released by anyone in the class.

Beyond the surprise of secondary uses of transparent information, the loss of practical obscurity also means that data aggregation and mining further enable the re-identification of otherwise anonymous individuals through predictive profiling.[51] One famous example is the identification of the author of Primary Colors—a political novel about the 1992 presidential election—who wrote under the name

51. *See generally* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

"Anonymous."[52] Data matching pinned the authorship to Joe Klein.[53] Similarly, Carnegie Mellon professor Latanya Sweeney has demonstrated in a number of works that re-identification from seemingly anonymous data streams is relatively simple.[54] According to other researchers at Carnegie Mellon, even Social Security numbers can be reverse engineered from publicly available data.[55] Paul Ohm has argued that the ease of re-identification undermines much of the protection afforded to individuals from existing American privacy law.[56]

The aggregation of data, thus, poses a dilemma for privacy. Dan Solove notes in his book *Understanding Privacy* that

> privacy may be implicated if one combines a variety of relatively innocuous bits of information. Businesses and government often aggregate a wide array of information fragments, including pieces of information we would not view as private in isolation. Yet when combined, they paint a rather detailed portrait of our personalities and behavior . . . .[57]

Solove has also highlighted that the Supreme Court recognizes the problem of privacy of public information. In *Department of Defense v. Federal Labor Relations Authority*,[58] a labor relations case, the Court said that "[a]n individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form."[59] Ironically, Justice Scalia was in the majority agreeing with this position.

G. Technological Nudity

In effect, the combination of these factors—network functionality, government programs, commercial pressures, security imperatives, social networking, and the loss of practical obscurity—lead to

---

52. ANONYMOUS AKA JOE KLEIN, PRIMARY COLORS (1996).

53. *Professor: Computer Finds Primary Colors Author*, CHI. TRIB., Feb. 16, 1996, at 2.

54. *See, e.g.*, Bradley Malin, Latanya Sweeney & Elaine Newton, *Trail Re-Identification: Learning Who You Are From Where You Have Been* (Carnegie Mellon Univ. Lab. for Int'l Data Privacy, Working Paper No. 12, 2003), http://dataprivacylab.org/dataprivacy/projects/trails/paper3.pdf.

55. Alessandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 PROCEEDINGS OF NAT'L ACAD. OF SCI. 10975 (2009).

56. *See generally* Ohm, *supra* note 51.

57. DAN SOLOVE, UNDERSTANDING PRIVACY 70 (2008).

58. U.S. Dep't of Def. *v.* Fed. Labor Relations Auth., 510 U.S. 487 (1994).

59. *Id.* at 500; SOLOVE, *supra* note 57, at 166.

extraordinary transparency in citizens' lives and create a form of technological nudity. Indeed, the Internet and network ecosystem erase the border between public and private information. The transparency expands the public space. Geolocating technologies and routine commercial uses reduce any expectations of privacy.

Normatively, the information society has created a "transparent citizenry." Citizens are widely exposed to public view without an effective boundary between public and private information. The transparent citizen loses informational self-determination in his or her relationship with the state and thus loses an important bedrock of democratic civil society.[60] Similarly, the transparent citizen's loss of informational self-determination alters his or her private relationships in society.

II. THE TRANSPARENCY CHALLENGE TO THE RULE OF LAW

The transparency of personal information presents a basic challenge to the rule of law both in terms of the state's faithfulness to its ideals and in terms of individuals' respect for its principles. The overexposure of citizens reduces the checks and balances on the exercise of government powers and diminishes citizens' trust and commitment to law.

A. Transparent Citizens and Non-Transparent Government

Typically, democracies shield the privacy of citizens from the state and make the activities of the state transparent.[61] In particular, democracy imposes specific limits on privacy intrusions by the state through legal and political mechanisms.

In the United States, both constitutional law and statutory requirements protect citizens from government acquisition of private information, but they are poorly adapted to the technological environment. The constitutional pillars for privacy rest on the First and Fourth Amendments. The First Amendment jurisprudence privileges

60. *See, e.g.*, Antoinette Rouvroy & Yves Poullet, *The Right to Informational Self–Determination and the Value of Self–Development: Reassessing the Importance of Privacy for Democracy*, *in* REINVENTING DATA PROTECTION? 45 (Serge Gutwirth et al. eds., 2009); Paul Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AM. J. COMP. L. 675 (1989); Spiros Simits, *Reviewing Privacy in a Surveillance Society*, 135 U. PA. L. REV. 707 (1987).

61. *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315 (2000) (discussing democracy's first principles in data privacy); *see also* Freedom of Information Act of 1966, 5 U.S.C. §552 (1966) (enshrining the principle of open government).

speech over privacy and imposes limits on privacy legislation.[62] The Fourth Amendment jurisprudence protects reasonable expectations of privacy that are now challenged by ubiquitous technology.[63]

The statutory framework is extensive and complex. Laws such as the Electronic Communications Privacy Act, the Right to Financial Privacy Act, and the Fair Credit Reporting Act restrain the state's ability to obtain information from private parties without a judicial check.[64] However, with respect to private parties, U.S. law tends to regulate the market process rather than provide a core, consistent set of substantive rights.[65]

Practical obscurity also provided an important political check on state data gathering and repurposing of public information. While much of the transparency of citizens comes from data that has long existed in disparate places, such as public property records or drivers' license records, or from data that could be acquired through surveillance in public places, the political and financial costs to hire investigators for every street corner who would observe and record citizens' movements were generally too high for democracy to justify such large scale data gathering campaigns.[66]

The technology driven data flows, however, invert democracy's traditional citizen-state relationship. Significant data processing functions and privacy invasive data mining by the state are now hidden from public view, while citizens' lives are now fully transparent to the state. This inversion undermines the carefully calibrated set of checks and balances on the state's acquisition and use of personal information. Transparent personal information erodes the Fourth Amendment boundary line. Ever since *Katz v. United States*,[67] the Supreme Court has protected privacy where there is a "reasonable expectation of

62. Sorrel v. IMS Health, 131 S. Ct. 2653 (2011) (striking down Vermont's protection for the prescription records of physicians).

63. *See* United States v. Jones, 132 S. Ct. 945 (2012); Kyllo v. United States, 533 U.S. 27 (2001); *see also* Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141 (2014).

64. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2012); Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 (2012); Fair Credit Reporting Act of 1968, 15 U.S.C. §§ 1681–1681t (2012).

65. *See* Reidenberg, *supra* note 61, at 1343–46.

66. See *Jones*, 132 S. Ct., at 963–64 (Alito, J., concurring) ("Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken."); Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 YALE L.J. ONLINE 335 (2014), http://yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones (showing historically diminishing costs of surveillance).

67. Katz v. United States, 389 U.S. 347 (1967).

privacy" against state intrusions. The transparent citizen, however, loses a reasonable expectation of privacy when information is in the public domain. In *Miller v. United States*, the Supreme Court held that a bank customer had no reasonable expectation of privacy in the information contained on a check because the check was disclosed to third parties while in circulation through the bank payment system.[68] Professor Christopher Slobogin makes the point that the government does not have to worry about the Fourth Amendment when it acquires data from government sources, commercial data brokers, or third-party businesses.[69] As Professor Danielle Citron has astutely observed, e-Government programs or "Government 2.0" enable the state to gather enormous amounts of information from citizens based solely on the public's access to government websites.[70]

Justice Scalia, writing for the Supreme Court in *Kyllo v. United States*, provides a technologically dependent view of the reasonable expectation of privacy.[71] While the Court held that the use of heat-sensing technology to recreate images of activity on the other side of a wall was a violation of the Fourth Amendment, Scalia wrote: "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[72]

The Court essentially ruled that because the technology was not in common use, the occupants of the home had a reasonable expectation of privacy against thermal imaging.[73] In other words, the common deployment of thermal-imaging technology would eliminate the reasonable expectation of privacy within the home.

Under this reasoning, the pervasive data collection and flow of the transparent citizen's personal information through ordinary, everyday technological interactions mean that citizens no longer have reasonable expectations of privacy. Indeed, with webcams deployed ever more frequently, the scope of one's reasonable expectation of privacy

68. Miller v. United States, 425 U.S. 435 (1976).

69. Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 330 (2008).

70. Danielle Keats Citron, *Fulfulling Government 2.0's Promise with Robust Privacy Protections*, 78 GEO. WASH. L. REV. 822 (2010); *see also* Angwin, *supra* note 22 (discussing the use of "'third party' tracking files" to gather detailed information about individuals that is then sold for advertising purposes).

71. Kyllo v. United States, 533 U.S. 27 (2001).

72. *Id.* at 40.

73. *Id.*

diminishes.

Beyond the problem of diminished reasonable expectations of privacy, government can effectively circumvent the checks and balances that protected citizen privacy by enlisting private intermediaries. Dan Solove notes that we have become a society of records held by third parties.[74] The transparent citizen makes it possible for government to act "sub rosa" through private intermediaries. Instead of seeking to collect information itself, government agencies buy data inexpensively from the commercial marketplace. For example, the Bush Administration's ill-fated, but not discarded, Total Information Awareness project ("TIA") sought to data mine information on millions of Americans. TIA caught William Safire's attention in a *New York Times* op-ed piece[75] and the outraged public response pressured Congress to curtail the program through spending appropriations restrictions.[76] Nevertheless, the program's surveillance goals were separately implemented in incremental steps, largely outside the public debate that surrounded TIA.[77]

When the federal government wanted information to profile pornography browsers on the Internet, it sent subpoenas to the five largest search engines asking the companies to provide their log files for all user search requests in a specific period of time.[78] The matter became public only when Google challenged the subpoena—the other search engine companies provided the data without objection.[79] Thus, the government's data surveillance was only accidentally revealed to the transparent citizens whose information was disclosed to the state. The alternative, wiretapping the net to mine traffic patterns, is something the government chose to avoid. It would have faced strict legal constraints, namely the need for search warrants for each of the individual account holders,[80] and inevitably public opposition like the outcry that occurred

74. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1089 (2002).

75. William Safire, *You Are a Suspect*, N.Y. TIMES, Nov. 14, 2002, at A35.

76. *See* Ira S. Rubinstein, Ronald D. Lee & Paul Schwartz, *Data Mining and Internet Profiling: Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 264 (2008).

77. *Id.* at 265.

78. Katie Hafner & Matt Richtel, *Google Resists US Subpoena of Search Data*, N.Y. TIMES Jan. 20, 2006, at A1.

79. *Id.* ("Google has been refusing the request since a subpoena was first issued last August, even as three of its competitors agreed to provide information, according to court documents made public this week.").

80. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

when the actual subpoenas were revealed.

Scholars have identified the problem of state-sponsored information surveillance. Jack Balkin refers to the use by government of publicly available information as the "National Surveillance State."[81] Patricia Bellia convincingly argues that online data retention policies feed indirect government surveillance.[82] James Dempsey and Lara Flint argue that commercial data mining for behavioral patterns turns the constitutional presumption of innocence around.[83] Christopher Slobogin, in his book *Privacy at Risk: The New Government Surveillance and the Fourth Amendment*, argues for legislative action to constrain government's use of transactional surveillance precisely because the Fourth Amendment does not recognize these data searches as constitutional violations.[84] The point is inescapable: the information-surveillance complex enables government to "search" citizens without the need for legal process or political accountability and the Fourth Amendment loses its protective value.

More recently, federal and state law enforcement agencies have established "fusion centers" throughout the country to facilitate the sharing of information among law enforcement agencies and homeland security.[85] Fusion centers combine data from online public sources and from private sector sources (e.g., purchased from data sellers and brokers). While the primary purpose for the creation of fusion centers in the post-9/11 period is to protect public safety, Danielle Citron and Frank Pasquale have aptly noted the troubling privacy implications.[86] The state can and does now engage in surveillance through data mining on individuals not suspected of any crime. Indeed, since the Winter Olympics in 2010, the U.S. government began a monitoring program for social media sites like Facebook and Twitter.[87] In other words, by mass

81. *See* Balkin, *supra* note 18, at 1.

82. Bellia, *supra* note 37, at 137.

83. James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459 (2004).

84. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007); Slobogin, *supra* note 37, at 107.

85. U.S. DEPT. OF JUSTICE, FUSION CENTER GUIDELINES: DEVELOPING AND SHARING INFORMATION IN A NEW ERA (2005), http://epic.org/privacy/fusion/report.pdf (describing the need for information sharing among public sector organizations and private sector companies).

86. Danielle Keats Citron & Frank A. Pasquale III, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441 (2011) (discussing the shortcomings of fusion centers and the need for network accountability to improve information sharing and stem the erosion of civil liberties).

87. Jason Ryan, *During the Olympics, the Feds Will Be Reading Your Tweets—and the Blotter*, ABC NEWS (Feb. 13, 2010), http://abcnews.go.com/Blotter/olympics-feds-reading-

collection and mining of social media data, the government presumes any citizen may be guilty rather innocent. Yet, the details of these programs are not readily found nor widely known. They are, simply put, non-transparent.

This transformation to non-transparent government surveillance represents an important shift and challenge for state respect for the rule of law. In the 1960s, when the federal government sought to computerize records for social security, Congress established the House of Representatives Special Subcommittee on Invasion of Privacy—a special subcommittee of the House Committee on Government Operations—because of concerns for the government's tracking and use of information about citizens.[88] Indeed, the Privacy Act of 1974 was enacted in the wake of Watergate and J. Edgar Hoover's domestic spying programs to bring government data processing out into the open. Or, as Justice Louis Brandeis once famously said, "sunshine is the best disinfectant."[89] Today, the pervasive, non-transparent state data collection activities that sidestep democratic checks and balances mean that public accountability will be diminished.

B. The Transparent Citizen and Commitment to Law

At the same time that the transparent citizen undercuts the state's faithfulness to the rule of law, transparency challenges private respect for the rule of law. Anonymity tools developed by the network community empower citizens to respond to the erosion of privacy. For example, cryptographic experts strive to create tamper-proof anonymity to protect against government watchfulness.[90]

But, anonymity tools have dual use. Just as they can protect against invasions of privacy, they also can empower and encourage wrongful behavior and the rejection of the rule of law. The Supreme Court has even recognized that "the right to remain anonymous may be abused when it shields fraudulent conduct."[91]

Wrongdoers use architectures of anonymity to try to evade the application of law to their activities. For example, JuicyCampus.com

---

tweets/story?id=9825070; Editorial, *Twitter Tapping*, N.Y. TIMES, Dec. 13, 2009, at WK8.

88. *Special Inquiry on Invasion of Privacy: Hearing Before the Special Subcomm. on Invasion of Privacy of the H. Comm. on Gov't Operations'*, 89th Cong., 2d Sess. (1966).

89. LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 29 (1914).

90. Sarah Spiekermann & Lorrie Faith Cranor, *Engineering Privacy*, 35 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 67, 72 (2009).

91. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).

was created to spread gossip and rumors about college students through anonymous postings on a website.[92] The site's business model was effectively based on the encouragement of posters to defame their classmates and hide behind the architecture of anonymity. AutoAdmit.com embodied a similar strategy.[93] More recently, in the business world, competitors have tried to wrongfully disparage their competition while hiding behind architectures of anonymity.[94]

Transparency also challenges the boundary between civic engagement and vigilantism. Perhaps the precursor is the 2007 website VideoVigilantes.blogspot.com, where short videos were posted to expose suspected wrongdoers who are caught on private webcams. Another interesting case study is the project launched in 2008 by the Texas Border Sheriff's Coalition. The coalition partnered with BlueServo to stream live images from webcams along the Mexican border as "an innovative real-time surveillance program designed to empower the public to proactively participate in fighting border crime."[95] The public is supposed to report suspected criminal activity to the sheriff, but at the same time, the data stream provides tools for those seeking to take justice into their own hands.[96] Even in the social arena, the dissemination on websites of comments designed to ostracize women and men[97] or to mark a virtual scarlet letter on college students

92. Sunny Hostin, *Online Campus Gossips Won't Show Their Faces*, CNN (Apr. 11, 2008), http://www.cnn.com/2008/CRIME/03/17/sunny.juicy/.

93. *See* Harold Hongju Koh, Dean, Statement to the Yale Law School Community on Malicious Website Postings (Mar. 8, 2007), https://www.law.yale.edu/yls-today/news/dean-harold-hongju-koh-statement-yls-community-malicious-website-postings (decrying the "racist, homophobic and other derogatory comments by anonymous posters" about Yale students); *see also* Steve Kolowich, *A New Gossip Guru*, INSIDE HIGHER ED (Feb. 25, 2011), http://www.insidehighered.com/news/2011/02/25/new_owner_of_college_gossip_website_collegeacb_promises_to_change_its_smear_culture (describing as ineffective changes to the website policies of http://www.collegeabc.com to limit disparaging material posted to the site and noting the site's architecture of anonymity).

94. *See, e.g.*, David K. Li, *Experts: No Cloak for 'Net Daggers*, N.Y. POST (Aug. 21, 2009, 7:04 AM), http://nypost.com/2009/08/21/experts-no-cloak-for-net-daggers/ (describing the problem faced by Liskula Cohen, a fashion model, who alleged that an anonymous blogger was defaming her on a blog as the "Skankiest in NYC").

95. *About BlueServo*, BLUESERVO, http://www.blueservo.net/about.php [https://web.archive.org/web/20130321024416/http://www.blueservo.net/about.php] (last visited Nov. 18, 2015).

96. *See, e.g.*, Christopher Ketcham, *The Angry Patriot*, SALON (May 11, 2005), http://www.salon.com/news/feature/2005/05/11/minuteman (discussing the Minuteman Project of citizen border patrols along the US-Mexican border).

97. *See* DON'T DATE HER DUDE, http://dontdateherdude.ning.com/ [https://web.archive.org/web/20111229093452/http://dontdateherdude.ning.com/] (last visited Nov. 18, 2015) (website designed to denigrate women); *See also* DON'T DATE HIM GIRL, http://dontdatehimgirl.com/home/ [https://web.archive.org/web/20130923134828/http://www.dontdatehimgirl.com/

who partied too hard[98] take on a vigilante character due to the permanence of the postings. If a tipping point in the malfeasant use of citizen transparency is reached, then general respect for the rule of law diminishes.

C. The Transparent Citizen and Public Safety

Even more significant than the challenge to respect for the rule of law, an overly transparent citizenry poses a basic threat to the existence of the rule of law in democratic society. Public safety is at risk from citizen transparency. The availability of too much information poses economic and physical threats. For example, a website, PleaseRobMe.com, illustrated that Twitter and Facebook postings could be used in conjunction with Google maps to show real-time information on homes that were vacant and easy to rob. Similarly, sites like HollaBackNYC.blogspot.com—a site designed to warn New York City women in real time of the location of harassers—may also mistakenly brand individuals. If adverse incidents multiply that are associated with transparent personal information, public fear of Internet disclosures will be harmful to society.

The transparent citizen also poses a national security risk that may threaten the very existence of the rule of law. Herb Lin of the National Academy of Sciences raises the specter that transparency may fuel cyber attacks by enemies.[99] Imagine that the now famous Scalia dossier—an organized collection of publicly available information profiling the Justice and his family members—is compiled for every flag officer in the United States military. The information could readily be used to create home life distractions during a military crisis. For example, simultaneous identity theft of officers across all military theaters of operation could be launched or could be launched against officers' immediate family members. Alternatively, information could be used to stalk or threaten officers' family members in coordinated attacks. Such attacks could wreak personal havoc for officers at precisely the moment when their undivided attention is needed for national security. The nation's economic security could similarly be threatened if an "information" attack were launched against the staff of

---

home] (last visited Nov. 18, 2015) (website designed to denigrate men).

98. *See* COLLEGE WALL OF SHAME, http://collegewallofshame.com/ (last visited Nov. 18, 2015) (anonymous posts of shameful photographs).

99. I am indebted to Herb Lin, Ph.D, chief scientist, National Academies of Science, for our discussion of this possibility.

major banks or stock exchanges simultaneously.[100]

D. The Transparent Citizen and Public Trust in Legal Institutions

Less dramatically, the transparent citizen also frames a challenge to the public's faith in legal institutions. In particular, the integrity of the judicial system is threatened by the transparency of personal information. Twittering lawyers and socially-networked judges may compromise faith in the fair administration of justice. When judges join social networks like LinkedIn or Facebook and affiliate with lawyers and litigants who appear before the court, perceptions of conflicts will arise.[101] Florida, for example, restricts judges' use of Facebook. A judge there may not ethically "friend" a lawyer who might appear before the judge.[102] The state's judicial ethics committee reasoned that "friending" would give the appearance of special influence.[103] Social media, similarly, may provide judges with the equivalent of ex parte communications should they receive updates on litigants or lawyers involved in cases before the court. But, simply wishing happy birthday to a judge might not qualify as an impermissible communication, at least in South Dakota.[104] At the same time, lawyers' use of social media exposes them to new twists on professional responsibility that can erode the public's trust in the profession. Lawyers' dubious behavior becomes widely known and representations to judges may be contradicted by online postings.[105]

Over-transparency may likewise infect the integrity of the jury

---

100. *Cf.* Nelson D. Schwartz & Christopher Drew, *RSA Faces Angry Users After Breach*, N.Y. TIMES, June 8, 2011, at B1 (mentioning that the hacker of RSA Security's databases was likely motivated by a desire to access military secrets through RSA's SecurID tokens, as several military contractors use them to protect their computer networks).

101. Debra Cassens Weiss, *Dozens of Judges are Getting LinkedIn, Blogger Notes*, A.B.A. J., (Aug. 20, 2009, 5:50 PM), http://www.abajournal.com/news/blogger_finds_dozens_of_judges_with_linkedin_profiles (last visited Nov. 13, 2015).

102. Fla. Sup. Ct. Judicial Ethics Advisory Comm., Op. 2009–20 (2009), http://www.jud6.org/LegalCommunity/LegalPractice/opinions/jeacopinions/2009/2009-20.html; *see also* Debra Cassens Weiss, *Judges Shouldn't 'Friend' Lawyers Who Appear Before Them, Opinion Says*, A.B.A. J. (Dec. 10, 2009, 1:22 PM), http://www.abajournal.com/news/article/judges_shouldnt_friend_lawyers_who_appear_before_them_opinion_says/.

103. Fla. Judicial Ethics Advisory Comm., Op. 2009–20.

104. *See* Onnen v. Sioux Falls Indep. Sch. Dist., 801 N.W.2d 752, 757–58 (S.D. 2011) (holding that a public message on Facebook wishing the judge a happy birthday did not require the judge to recuse himself from the case).

105. *See* Molly McDonough, *Facebooking Judge Catches Lawyer in Lie, Sees Ethical Breaches #ABAChicago*, A.B.A. J., (July 31, 2009, 816: PM), http://www.abajournal.com/news/article/facebooking_judge_catches_lawyers_in_lies_crossing_ethical_lines_abachicago (last visited Nov. 18, 2015).

system. Jury selection can readily be contaminated by search engine digging into the lives of potential jurors. In one famous case, Judge Coar banned lawyers from using Google to learn about jurors outside the court.[106] Many lawyers also search social media sites for information on potential jurors.[107] Jury service may similarly be tainted by a juror who, unbeknownst to the attorneys or judge, uses search engines to find extra information about the people involved in the case. The Supreme Court of South Dakota, for example, threw out a jury verdict in the case of a "Googling juror."[108]

III. THE TRANSPARENCY CHALLENGE TO INTERNATIONAL NORMS AND DATA FLOWS

The transparent citizen through ubiquitous and ambient data gathering likewise presents a challenge to international norms and data flows. In essence, the transparent citizen creates an international legal problem. Like the situation in the United States, existing foreign norms are pushed to the limits, and the legal instruments designed to assure the respect for privacy and to allow transborder data flows between different legal systems lose stability.

A. The International Legal Problem

Throughout the world, data privacy laws create a legal framework for the processing of personal information.[109] As Neil Richards argues, intellectual privacy, or the protection of personal information needed to formulate one's thoughts and develop one's associations, is essential for democracy.[110] These laws thus reflect an international consensus on basic fair information practice principles for democracies that dates back to the 1980s with the promulgation of the *OECD Guidelines on*

106. Rudolph Bush & Michael Higgins, *Judge Bans Juror Checks*, CHI. TRIB., Apr. 27, 2006, at 2C.1.

107. *See* Ana Campoy & Ashby Jones, *Searching for Details Online, Lawyers Facebook the Jury*, WALL ST. J., Feb. 22, 2011, at A2.

108. Russo v. Takata Corp., 774 N.W.2d 441, 441–44, 454 (2009) (holding that the trial court did not abuse its discretion when it granted the plaintiff's motion for a new trial due to a juror's performance of a Google search of the defendant Takata Corp); Thomas O'Toole, *Googling Juror Prompts Court to Overturn Jury Verdict*, BLOOMBERG BNA: TECH., TELECOMM. & INTERNET BLOG (Sept. 18, 2009), http://www.bna.com/googling-juror-prompts-b12884907079/.

109. *See, e.g.*, EU Council Directive 95/46, *supra* note 47, art. 9, (establishing legal requirements for data privacy throughout Europe); PABLO A. PALAZZI, LA TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES Y LA PROTECCIÓN DE LA PRIVACIDAD (2002) (discussing Latin American data privacy laws); PETER BLUME, NORDIC DATA PROTECTION LAW (2001) (discussing Nordic countries' data privacy laws).

110. NEIL RICHARDS, INTELLECTUAL PRIVACY (2015).

Privacy and the Transborder Flows of Personal Data[111] and the Council of Europe's *Convention for the Protection of Individuals with Regard to Automatic Processing Personal Data*.[112] The norms elaborated in these instruments seek to define fairness in the collection, use, and storage of personal information. While these instruments are international, data privacy law exists as a matter of national law.

At the core, however, national data privacy law is deeply anchored in each country's constitutional culture.[113] Outside the United States, most countries approach privacy with a strong, comprehensive national law grounded in the conception of privacy as a fundamental human right.[114] On the books, these laws appear to offer stronger protection than U.S. law where privacy is seen more as a market regulated value; but, in practice, the effects of comprehensive data privacy laws often fall short of their aspirations.[115]

Just as the U.S. legal framework faces challenges from the transparency of citizens' personal information, foreign data protection laws also face overload. The European Union's data privacy framework provides a key illustration. European countries express key political values through the evolution of their data privacy regimes. In the post-WWII period, European countries began an economic integration process with the formation of the European Coal and Steel Community[116] and expanded efforts to create a single economic marketplace with the Single European Act[117] and the Treaty on European Union.[118] During this time, various European countries including France, Germany, and the United Kingdom responded to the

111. OECD, *Guidelines*, *supra* note 47.

112. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, C.E.T.S. 108, http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm; *see* Reidenberg, *supra* note 61, at 1343–46; *see also* Paul M. Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1969–71 (2013).

113. Reidenberg, *supra* note 112.

114. This is the model from the Council of Europe's convention that has been highly influential around the world, first in Europe with the adoption of Directive 95/46/EC and then followed in Latin America and elsewhere.

115. Dierdre Mulligan & Kenneth Bamberger, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*, 81 GEO. WASH. L. REV. 1529 (2013); Dierdre Mulligan & Kenneth Bamberger, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2010).

116. *See* Treaty Establishing the European Coal and Steel Community, EUR., Apr. 18, 1951, 261 U.N.T.S. 11, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:xy0022.

117. Single European Act, Feb. 17, 1986 O.J. (L 169), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1987:169:FULL&from=EN.

118. Treaty on European Union, Feb. 7, 1992 O.J. (C 191), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012M/TXT&from=EN.

computerization of their societies with data privacy legislation. By 1995, following the Single European Act, Europe sought to harmonize data privacy legislation to promote a pan-European internal market for information services. Yet, as European integration took on a greater political dimension with further treaties culminating in the Treaty of Lisbon,[119] data privacy became a core European political right enshrined in the Charter of Fundamental Rights of the European Union.[120] Indeed, the current data protection reform serves an important governance function. The draft General Data Protection Regulation ("GDPR")[121] provides a centralization of data privacy law at the European level and enshrines privacy as a pan-European political right.

And, more precisely, Europe is grappling directly with the transparent citizen problem. For example, both the GDPR and the Court of Justice of the European Union have sought to articulate a "right to be forgotten"[122] for automatically processed data. The GDPR is also seeking to match political rights to new economic issues such as profiling,[123] data security breach,[124] and corporate responsibility.[125] Europe looks at citizen transparency from the perspective of privacy as a fundamental right.

B. International Instability

To avoid the circumvention of European protections, EU law prohibits the transfer of personal data to countries that fail to provide an "adequate" level of privacy protection.[126] As a result, the underlying and national political conceptions of data privacy law create instability for international data flows. Trade conflicts over privacy in the private

---

119. Treaty of Lisbon, Dec. 13, 2007, O.J. (C 306), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12007L/TXT&from=EN.

120. Charter of Fundamental Rights of the European Union, Dec. 14, 2000, O.J. (C 364/1), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2007:303:FULL&from=EN.

121. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation*), SEC (2012) 73 final (Jan. 25, 2012) [hereinafter *General Data Protection Regulation Proposal*].

122. *Id.* at 20; *see also* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN [http://perma.cc/ED5L-DZRK].

123. *General Data Protection Regulation Proposal*, *supra* note 121, at 20.

124. *Id.* at 22.

125. *Id.* at 30.

126. Council Directive 95/46, *supra* note 47, art. 25.

sector have created significant uncertainty over the years.[127] Similarly, political conflicts over privacy in the public sector have challenged data flows such as the disputes over data gathering and mining for national security.[128] Outside of Europe, similar handwriting appears on the walls. Brazil, for example, considered a data localization rule that would require local processing of Brazilian data in order to protect its views of citizens' privacy.[129]

To facilitate data flows across the different legal systems, various international bridges between the U.S. and Europe have evolved. In particular, in order to satisfy the "adequacy" standard in EU law for data exports, three mechanisms emerged: the U.S.-EU Safe Harbor, Binding Corporate Rules, and Model Contracts.[130] These solutions, however, do not resolve conflicts between the legal systems' underlying choices. For example, as Paul Schwartz and Daniel Solove argue, the solutions do not address fundamental differences between Europe and the U.S. on the meaning of "personal information," which is critical for the applicability of protections.[131] Similarly, in the wake of the Snowden disclosures, the European Parliament challenged the viability of the Safe Harbor.[132]

C. Political Choices and Stability

The transparent citizen forces inherent political choices to the forefront if privacy is to be effectively protected in a globally networked

---

127. *See, e.g.*, PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE AND THE EUROPEAN PRIVACY DIRECTIVE 188–96 (1998) (discussing privacy as a trade clash).

128. *See* Commission de la Protection de la Vie Privee [CPVP], AV37-2006 (Sept. 27, 2006) (Belg.) (examining the sharing of wire transfer information by SWIFT with the US government); Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, EU-U.S., Dec. 8, 2011 O.J. (L 204) (authorizing the exchange of airline passenger information from air carriers in Europe to the U.S. government); Press Release, European Committee on Civil Liberties and Committ on Justice and Home Affairs, US NSA: Stop mass surveillance now or Face Consequences MEPs Say (Mar. 12, 2014) [hereinafter MEP Statement] http://www.europarl.europa.eu/pdfs/news/expert/infopress/20140307IPR38203/20140307IPR38203_en.pdf.

129. Allison Grande, *Brazil Nixes Data Localization Mandate From Internet Bill*, LAW360 (Mar. 20, 2014), http://www.law360.com/articles/520198/brazil-nixes-data-localization-mandate-from-internet-bill.

130. *See* Paul M. Schwartz, *The EU-U.S. Privacy Collision*, 126 HARV. L. REV. 1966, 1980–84 (2013).

131. *See* Paul M. Schwartz & Daniel Solove, *Reconciling Personal Information in the United States and Europe*, 102 CALIF. L. REV. 877, 879 (2014) (arguing that international data transfer mechanisms are unstable because of different views of "personally identifiable information").

132. *See* MEP Statement, *supra* note 128; Schwartz, *supra* note 130, at 1984.

environment. The transparent citizen re-engages society in the definition of the role of the state in governing information flows. States must re-confront the political choice of protecting privacy as a fundamental right or protecting information as an economic commodity. In effect, the choice is a profound decision on each state's organizing principles: do privacy rights serve as a bulwark against state power or do privacy rights empower a state to check private authority?

A lack of uniformity across borders is likely. Different societies will make different decisions based on their constitutional heritages about the role of the state and the purpose of privacy rights. This lack of uniformity assures that there will be continued conflict for international data flows that are political in nature.

Traditionally, nation-state political conflicts are resolved by international treaties. Privacy will not be an exception. In fact, since the mid-1990s, privacy has appeared in international trade treaties.[133] The resolution of core, underlying political differences on privacy and the state's role will need an international legal instrument to create transborder data flow stability. At the moment, the trade framework appears first on international agendas.[134] Yet, the trade approach favors the commodity conception of privacy rather than the fundamental right philosophy.[135] Since the trade treaty negotiations are conducted in secret by government representatives for economic actors, the political differences over non-economic values risk being short shrifted and, as Margot Kaminski argues, need a full public airing outside the trade arena where privacy will be bundled with other issues.[136]

IV. CONCLUSION

The transparent citizen forces democracies to confront a crucial question for a globally connected, information-dependent world: what kind of open society do we want to have? To have an open, democratic

133. Reidenberg, *supra* note 112, at 1359–62.

134. *See, e.g.*, Draft Trade in Services Agreement (TiSA) Annex on Electronic Commerce, art. 4, Sept. 16, 2013, https://wikileaks.org/tisa/ecommerce/TiSA%20Annex%20on%20Electronic%20Commerce.pdf.

135. Reidenberg, *supra* note 112, at 1361 ("Although, pursuing a WTO strategy places data protection in the trade arena rather than a political arena, WTO increasingly faces the incorporation of noneconomic values in trade policy."); Margot E. Kaminski, *Privacy is not a Barrier to Trade*, SLATE (June 4, 2015), http://www.slate.com/articles/technology/future_tense/2015/06/trade_in_services_agreement_could_change_the_global_internet.html.

136. *See* Margot E. Kaminski, *Why Trade is not the Place for the EU to Negotiate Privacy*, INTERNET POL'Y REV. (Jan. 23, 2015), http://policyreview.info/articles/news/why-trade-not-place-eu-negotiate-privacy/354 (arguing against the trade approach).

society, citizen transparency needs to be checked. Our challenge going forward is whether and how we can craft legal and technical instruments to re-instantiate obscurity for citizens' information.