LESSONS LEARNED TOO WELL: ANONYMITY IN A TIME OF SURVEILLANCE

A. Michael Froomkin*

It is no longer reasonable to assume that electronic communications can be kept private from governments or private-sector actors. In theory, encryption can protect the content of such communications, and anonymity can protect the communicator's identity. But online anonymity—one of the two most important tools that protect online communicative freedom—is under practical and legal attack all over the world. Choke-point regulation, online identification requirements, and data-retention regulations combine to make anonymity very difficult as a practical matter and, in many countries, illegal. Moreover, key internet intermediaries further stifle anonymity by requiring users to disclose their real names.

This Article traces the global development of technologies and regulations hostile to online anonymity, beginning with the early days of the Internet. Offering normative and pragmatic arguments for why communicative anonymity is important, this Article argues that anonymity is the bedrock of online freedom, and it must be preserved. U.S. anti-anonymity policies not only enable repressive policies abroad but also place at risk the safety of anonymous communications that Americans may someday need. This Article, in addition to providing suggestions on how to save electronic anonymity, calls for proponents of anti-anonymity policies to provide stronger justifications for such policies and to consider alternatives less likely to destroy individual liberties. In a time where

---

* Laurie Silvers & Mitchell Rubenstein Distinguished Professor University of Miami School of Law. This paper has gone through a number of iterations. Earlier versions benefitted from feedback at "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" at the Oxford Internet Institute in 2011, the 5th Annual Privacy Law Scholars Conference in 2012, and the Freedom of Expression Scholars Conference at Yale Law School 2015, as well as at workshops organized by the Yale ISP, and by New York Law School. I would like to thank Caroline Bradley for years of patience, Chase Smith and Steven Strickland for research assistance, and Jose Ponce for assistance, especially with developments in Latin America and translations from Spanish. I also owe an enormous debt to the University of Miami Law School's excellent reference librarians. Errors remaining despite all this assistance, and that of many other faculty colleagues as well, are my own. Unless otherwise noted, this article attempts to reflect legal and technical developments through November 2016.

surveillance technology and laws demanding identification abound, protecting the right to speak freely without fear of official retribution is critical to protecting these liberties.

TABLE OF CONTENTS

INTRODUCTION

We live in a time of surveillance. In a trend that began some time ago,[1] but now seems to be accelerating, surveillance is becoming pervasive in both physical space and in electronic communications.[2] Recent responses to terrorist attacks in Marseille, Paris, New York, and at the Boston Marathon exacerbated—or provided excuses to escalate—the move towards pervasive surveillance. Twenty years ago, we were entitled to assume that our electronic communications were private. Communications privacy was the default rule, and deviations from that default required, in most cases, either a lawful subpoena in connection with a

1. *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1472–1501 (2000) (warning of the dangers of the pervasive collection of physical and online data).

2. *See generally* A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 ILL. L. REV. 1713 (proposing a solution to address the problem of pervasive data collection).

criminal investigation or someone with technical sophistication and the willingness to break the law.

Today, the evidence points exactly the other way: a reasonable person should assume that every electronic communication is being captured by one or more governments, and that many, if not most or all, electronic communications are likely accessible, in whole or in (metadata) part, to various private actors.[3] This new default rule has not yet become an ironclad rule: it remains possible, perhaps, to safeguard one's electronic and personal privacy but only with greater and greater effort. In the case of electronic communications, the two means of preserving or reclaiming our privacy are encryption and anonymity. Encryption directly protects the content of communications but does not necessarily obscure facts about who is communicating with whom, when, and where.[4] Anonymity protects the identity of the sender of a communication and, at times, even the recipient of that communication. Cryptography is necessary, but not sufficient, for strong anonymity online.

The election of Donald Trump likely raises the stakes on anonymous communications in the United States.[5] The more pervasive surveillance becomes, the more the right to communicate anonymously grows in importance as a rare form of free, unmonitored communication. The government's willingness to use the fruits of existing surveillance may grow also, making the consequences of being surveilled more serious. If so, the ability to communicate anonymously will become ever more essential—and more likely to come under further sustained assault.

In theory, the right to communicate anonymously is protected by U.S. law and, arguably, by some international human-rights norms as well. In practice, the ability to communicate anonymously is under sustained legal and practical attack,

---

3. A major driver of this phenomenon is the rapidly decreasing cost of surveillance. *See, e.g.*, 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, 341 (2014).

4. *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PENN. L. REV. 709 *passim* (1995). For a survey of legal restrictions on cryptography, see generally Nathan Saper, *International Cryptography Regulation and the Global Information Economy*, 11 NW. J. TECH. & INT'L PROP. 673 (2013).

5. Although Trump's election occurred while this Article was in proof, many commentators have provided early warnings of the implications for anonymous communications. *See, e.g.*, Joseph Cox, *Could President Trump Really Turn the NSA Into a Personal Spy Machine?*, MOTHERBOARD (Nov. 9, 2016, 12:14 PM), http://motherboard.vice.com/read/could-president-trump-really-turn-the-nsa-into-a-personal-spy-machine; Thomas Fox-Brewster, *Scared About Trump Wielding FBI and NSA Cyber Power? You Should Be*, FORBES (Nov. 9, 2016, 1:00 PM), http://www.forbes.com/sites/thomasbrewster/2016/11/09/donald-trump-president-of-fbi-nsa-surveillance-state/#7a77b0db7b19; Jon Stokes, *How President Trump Could Abuse Big Data and the Surveillance State*, TECHCRUNCH (Nov. 13, 2016), https://techcrunch.com/2016/11/13/how-president-trump-could-abuse-big-data-and-the-surveillance-state/.

both in the United States and around the world. This Article examines how that came to be, why it matters, and possible solutions. The focus here is on internet communications at the expense of telephony. This is because unlike both wired and wireless telephony systems, which are designed with built-in identifiers for billing and routing, the Internet's technical architecture is compatible with anonymity.[6]

A decade ago, the Internet was already subject to a significant degree of national regulation. This first generation of internet law was somewhat patchy and often reactive. Some legal problems were solved by simple categorization, whether by court decisions, administrative regulation, or statute. Other problems required new approaches: the creation of new categories (often judicial) or of new institutions (often private). And in some cases, governments in the United States and elsewhere brought out the big guns of legislation, sometimes with stiff penalties.

The past decade has seen the crest of the first wave of regulation and the gathering of a second, stronger wave based on a better understanding of the Internet and of law's ability to shape and control it. Aspects of this second wave are encouraging. Internet regulation is increasingly based on a sound understanding of the technology, minimizing pointless rules or unintended consequences. But other aspects are very troubling. Where a decade ago it was still reasonable to see internet technologies as empowering and anti-totalitarian, regulators in both democratic and totalitarian states have now learned to structure rules that current techniques cannot easily evade, leading to previously impossible levels of regulatory control.

On balance, that trend seems likely to continue; at the very least, the risk that it will do so is very real. One likely result of current trends in centralization and smarter, more global regulation is the legal restriction, and perhaps prohibition, of online anonymity. As a practical matter, the rise of identification technologies combined with commercial and regulatory incentives has made it difficult for anyone other than the most sophisticated users to remain effectively anonymous. First-wave internet regulation could not force the identification of every user and packet, but the second-wave regulation is more adept and more international, and it benefits from technological change driven by synergistic commercial and regulatory objectives. Law that harnesses technology to its ends achieves far more than law regulating around technology or against it.

Part I of this Article discusses the first wave of internet regulation, enacted before the year 2000, focusing on U.S. law. This narrow focus is excusable because even at the start of the twenty-first century a disproportionate number of internet users were in the United States.[7] And, with only a very few

---

6. Telephony, however, is rapidly moving to VoIP—Internet telephony. *See, e.g.*, *VoIP, Unified Communications Markets Set for Massive Growth*, AKKADIAN LABS (Nov. 18, 2014), http://www.akkadianlabs.com/voip-unified-communications-markets-set-for-massive-growth/.

7. In 2000, the United States had almost twice as many internet users as the next highest country, Japan, and almost as many internet users as Japan, Germany, and China combined. *See The Incredible Growth of the Internet Since 2000*, PINGDOM: TECH

exceptions—the greatest of which involve aspects of privacy law emanating from the European Union's Privacy Directive[8]—the United States either led or at least typified most of the first-wave regulatory developments.

The second wave of regulation has been much more global. Therefore, in Part II, which concerns the most recent decade and a half, this Article's focus expands geographically but narrows to specifically anonymity-related developments. Section II.A describes private incentives and initiatives that resulted in the deployment of a variety of technologies and private services, each of which is unfriendly to anonymous communication. Section II.B looks at three types of government regulation relevant to anonymity: (1) the general phenomenon of choke-point regulation; (2) the more specific phenomena of online identification requirements; and (3) data retention (which can be understood as a special form of identification).

Part III examines competing trends that may shape the future of anonymity regulation. While the Snowden revelations play a part in this account, they do not occupy the entire stage. One of the key objectives of this Part is to show how technologies of identification, only some of which are driven by national-security concerns, are being baked into technology by law. Indeed, this Part argues that, given the rapid pace of technical and regulatory changes, the fate of online anonymity in the next decade will be determined by the deployment of new technologies or, most likely, pragmatic political choices, rather than by law. It therefore offers normative and pragmatic arguments regarding why anonymity is worth preserving and concludes with questions that proponents of further limits on anonymous online speech should be required to address.

Goaded by factors ranging from traditional public order concerns to fear of terrorism and hacking to public disclosures by WikiLeaks and others, both democratic and repressive governments are increasingly motivated to identify the owners of every packet online, and to create legal requirements that will assist in that effort. Yet whether a user can remain anonymous or must instead use tools that identify him is fundamental to communicative freedom online. One who can reliably identify speakers and listeners can often tell what they are up to even if he is not able to eavesdrop on the content of their communications; acquiring the content itself only makes the intrusion and the potential chilling effects that much greater. Content industries with copyrights to protect, firms with targeted ads to market, and governments with law enforcement and intelligence interests to promote all now appreciate the value of identification, and the additional value of traffic analysis, not to mention the value of access to content on demand—or even the threat of it.

Online anonymity is closely related to a number of other issues that contribute to communicative freedom, and thus enhance civil liberties. These

---

BLOG (Oct. 22, 2010) http://royal.pingdom.com/2010/10/22/incredible-growth-of-the-internet-since-2000/.

8. *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 OJ (L 281) 31 [hereinafter EU Data Directive].

include the free use of cryptography and the use of tools designed to circumvent online censorship and filtering. One might reasonably ask why, then, this Article concentrates on anonymity and on its inverse, identification technologies. The answer is that anonymity is special—arguably more essential to online freedom than any other tool except perhaps cryptography (and one of the important functions of cryptography is to enable or enhance anonymity as well as communications privacy). Without the ability to be anonymous, the use of any other tool, even encrypted communications, can be traced back to the source. Gentler governments may use traffic analysis to piece together networks of suspected dissidents, even if the government cannot acquire the content of their communications. Less-gentle governments will use less-gentle means to pressure those whose communications they acquire and identify. Regardless of whether anonymity is sufficient to permit circumvention of state-sponsored communications control, it is necessary to ensure that those who practice circumvention in the most difficult circumstances have some confidence that they may survive it.

The consequences of an anonymity ban are likely to be negative. What follows attempts to explain how we came to this pass, and what should be done to avoid making the problem worse.

I. THE FIRST WAVE OF INTERNET REGULATION

A. Precursors

The Morris worm of November 1988 serves now as a reminder of how internet regulation worked before we had internet regulation. On November 2, 1998, Robert Morris Jr., then a Cornell graduate student, unleashed a self-replicating, self-propagating computer program on the Internet. He had intended his experiment to copy itself slowly, but a coding error caused it to replicate so quickly that it brought infected machines to a halt. Indeed, the "worm" caused such great network congestion that it blocked subsequent messages he sent out with instructions on how to kill the worm and prevent its re-emergence.[9]

Despite the novelty of the problem, the ordinary legal system found a way to deal with the graduate student who accidentally unleashed the first widely-deployed internet pest: Robert Morris, Jr. was convicted of violating the Computer Fraud and Abuse Act of 1986[10] and sentenced to three years of probation, 400 hours of community service, and a fine of $10,050 plus the costs of his supervision.[11] No new law was needed to prohibit and sanction Morris's conduct. But a raft of new laws would soon be coming.

By 1990, the Internet was already past its toddler years and on the cusp of a precocious adolescence. Early internet users tended to be academics, engineers, hobbyists, and hackers—"hackers" in the nicest possible sense of the term as they were people who played with tools, not people who broke things or even, in the

9. BRENDAN P. KEHOE, ZEN AND THE ART OF INTERNET 61–62 (1st ed. 1992).

10. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1986 § 2, 18 U.S.C. § 1030(a) (1988).

11. United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991).

main, broke into things.[12] While researchers and specialists often relied heavily on Unix-based machines,[13] the majority of nonspecialist users used computers running DOS,[14] Windows 3.1,[15] or the Apple Macintosh.[16] Most online interactions were still text based; graphics tended to be attachments, files to download, or maybe ASCII art.[17] The search for serious reference material sometimes required recourse to gopher space.[18] There were many "walled gardens" like AOL.[19]

The first web server apparently dates to August 1991. The first web-based photo, an image of the European Organization for Nuclear Research house band

---

12. *See generally* KATIE HAFNER & MATHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (1998) (describing key players in creating ARPANET and the formation of the early Internet).

13. Unix is a family of computer operating systems, derived from the original AT&T Unix invented in Bell Labs, that are suitable for multitasking, multiuser systems, or for stand-alone machines on a network. The name is said to be a pun in that Unix was an emasculated Multics. Among Unix's characteristics are a modular structure and strong security model. Unix-based systems were popular with the software engineers who first developed or gravitated towards the internet. *See* PETER H. SALUS, A QUARTER-CENTURY OF UNIX 1–9 (1994).

14. DOS, or "Disk Operating System," was the operating system shipped with the original IBM personal computers. IBM first shipped PC-DOS then switched to MS-DOS, or "Microsoft Disk Operating System," for the IBM PC-XT. *See Microsoft MS-DOS Early Source Code*, COMPUTER HIST. MUSEUM (Mar. 25, 2014), http://www.computerhistory.org/atchm/microsoft-ms-dos-early-source-code/.

15. Windows XP was not introduced until August 24, 2001. *See Windows XP to Take the PC to New Heights*, MICROSOFT (Aug. 24, 2001), https://news.microsoft.com/2001/08/24/windows-xp-to-take-the-pc-to-new-heights/#sm.00003rrbap1ej2f9tyvqeb11jljwf#lucZ64qOMmMwcZMJ.97.

16. Apple started selling the Macintosh in 1984; by 1987 Apple was selling one million (upgraded) Macintoshes per year. Christopher Dernbach, *The History of the Apple Macintosh*, MAC HISTORY, http://www.mac-history.net/top/2011-01-24/the-history-of-the-apple-macintosh (last visited Jan. 31, 2017).

17. The American Standard Code for Information Interchange ("ASCII") is a standard for encoding alphanumeric and other characters as a seven-bit binary number (a string of seven zeros or ones). It is the most common format for text files in computers and on the Internet. *See* Mary Brandel, *1963: The Debut of ASCII*, CNN.COM (July 9, 1999, 12:48 PM), http://edition.cnn.com/TECH/computing/9907/06/1963.idg/. ASCII Art is a form of representing graphics on monitors or printers using only ASCII characters—a workaround necessitated by the absence of graphics capabilities on most early computer monitors and dot-matrix printers. Christopher Johnson, *What is ASCII Art?*, CHRIS.COM, http://www.chris.com/ascii/index.php?page=what-is-ascii-art (last visited Jan. 16, 2017).

18. University of Minnesota researchers developed the Gopher Protocol in 1991 to organize and share documents over the Internet. Originally a text-based method of browsing the Internet, Gopher allowed users to access documents through a menu-driven hierarchical system. *See* Nate Anderson, *The Web May Have Won, but Gopher Tunnels On*, ARS TECHNICA (Nov. 4, 2009, 6:15 AM), http://arstechnica.com/tech-policy/news/2009/11/the-web-may-have-won-but-gopher-tunnels-on.ars.

19. *See* M. Scott Boone, *The Past, Present, and Future of Computing and Its Impact on Digital Rights Management*, 2008 MICH. ST. L. REV. 413, 421 n.47 (defining the term "walled garden" as "a network . . . that restricts its users to its own content").

Les Horribles Cernettes, is said to date to 1992,[20] but most of us who were online then primarily used email, mailing lists, USENET, or maybe a text-based web browser like Lynx. Some of the cooler folks were exploring text-based online virtual reality systems like MUDs ("multiple user dungeons") and MOOs ("MUD, object oriented"), or early social sites like the WELL ("Whole Earth 'Lectronic Link").[21]

If you wanted to get into this world of computer-mediated interaction, you either went to graduate school in computer science, found someone to teach you, or bought (not downloaded) a book: *The Whole Internet User's Guide And Catalog*.[22] During the '90s, a million people bought that book,[23] even though a downloadable version was available from the publishers as early as 1993—but only as a demo of the Global Network Navigator, an early browser which very few were then able to use.[24]

In 1990, basically no targeted internet law existed as such, although there was, of course, a lot of law that could apply to people who used the Internet, just as it applies to people who use any other tool. Most internet connections between computers ran over telephone lines, with the last mile of connection starting with a modem or perhaps a very local network. The Bell System's monopoly on what could be connected to telephones had been broken,[25] so the heavy hand of its contracts was as absent as that of the Federal Communications Commission ("FCC"). There was, however, a great deal of critical self-regulation not just at the protocol level in the form of the Requests for Comments ("RFCs")[26] issued by the Internet Engineering Task Force ("IETF"), but also in the management of common user forums like USENET.[27]

---

20. Silvano de Gennaro, *A Page of History*, http://musiclub.web.cern.ch/MusiClub/bands/cernettes/firstband.html (last visited Jan. 16, 2017).

21. The Whole Earth 'Lectronic Link ("WELL") is one of the oldest online communities on the Internet, beginning as a dial-up bulletin board system and evolving with web-browsing technological developments. Ron Pernick et al., *A Timeline of the First Ten Years of The WELL*, WELL (1995), http://www.well.com/conf/welltales/timeline.html.

22. *See generally* ED KROL, THE WHOLE INTERNET USER'S GUIDE AND CATALOG (1st ed. 1992).

23. *The Whole Internet User's Guide & Catalog*, ARCHIVE.ORG, http://www.archive.org/details/wholeinternet00krolmiss (last visited Jan. 16, 2017).

24. *See* Tim O'Reilly, *History & Company Overview from President*, LANDLEY.NET, http://www.landley.net/history/mirror/perl/tim.html; *see also* Tim O'Reilly, *Giving Away Free Books*, O'REILLY (Nov. 30, 2000), http://archive.oreilly.com/pub/a/oreilly/tim/articles/wolfe-gnn.html (relating the story of the Global Network Navigator).

25. *See* United States v. Am. Tel. & Tel. Co., 552 F. Supp. 131 (D.D.C. 1982), *aff'd sub nom.* Maryland v. United States, 460 U.S. 1001 (1983).

26. RFCs are the documentation of internet standards. The name arose because the original designers of the Internet were graduate students and wanted to make clear they were not claiming any authority for fear of retribution from whoever the real authorities might be. *See* A. Michael Froomkin, *Habermas@discourse.net: Toward a Critical Theory of Cyberspace*, 116 HARV. L. REV. 749, 784 (2003).

27. *See generally id.*

This extensive and generally effective self-regulation dovetailed with, and indeed fed, an ethos of empowerment and, at least in the minds of its adherents, optimism. It would later feed into the anti-regulatory idea that the Internet should be treated as a legally autonomous area, but that never caught on, nor did it deserve to.

The packet switching that underlies the Internet famously decentralizes communication and makes censorship difficult—hence, the first part of the optimists' credo, now almost a cliché: "The Net interprets censorship as damage and routes around it."[28] Even worse from the censor's point of view, strong cryptography was now available to the masses for the price of a download—that is, free unless you had to pay for your phone connection.

Packet switching plus strong cryptography seemed to herald total communicative freedom. And to the libertarian-leaning types[29] who were greatly overrepresented in the early online community, that sounded really good. Among the things this new freedom promised were decentralization, lower transaction costs, and the empowerment of the periphery over the center. Thus the optimistic enthusiasts predicted a number of goodies:

- The replacement of the one-to-many model by a many-to-many model.
- A globalized, decentralized, subsidiarity-loving, empowered, mass culture, in which news and information flows would move chaotically around the network rather than down the narrow channels of mass media and centralized opinion formation.
- New online communities, allowing widely scattered groups to coalesce ranging from the "World Union of Concerned Butterfly Fanciers" to global diasporic communities.
- Enhancement of democracy via better citizen information, better communication with government, and, especially, via better organization of citizens groups and NGOs.
- The spread of anti-censorship software, proxies, and the use of anonymizing browsers or cryptographically enhanced "tunneling" software in such profusion that no government would be able to prevent information from entering on internet-enabled networks. Thus is the appeal

28. The quote is attributed to John Gilmore, co-founder of Electronic Frontier Foundation. Richard Rogers, *The Internet Treats Censorship as a Malfunction and Routes Around It?*, *in* THE SPAM BOOK 243 (Jussi Parikka & Tony D. Sampson eds., 2009).

29. An important sub-group of libertarian cryptographers and coders styled itself the Cypherpunks. *See* THOMAS RID, RISE OF THE MACHINES 246–93 (2016); Eric Hughes, *A Cypherpunk's Manifesto*, ELECTRONIC FRONTIER FOUND. (Mar. 9, 1993), https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto (last visited Jan. 16, 2017); Timothy C. May, *The Cyphernomicon* (Sept. 10, 1994), [hereinafter *The Cyphernomicon*] https://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.txt.

of the catchphrase "information wants to be free."[30] (To which the copyright owners would soon respond, "No, information wants to be paid for."[31])

- Regulatory arbitrage: to the extent that things of value (information, some services, stocks and soon, it was confidently believed, currency) could be digitized, they could be traded and moved across borders to the regime with the most attractive regulatory climate.[32] Thus the appeal of the other catchphrase: "national borders aren't even speed bumps on the information superhighway."[33]

For those who saw much more good than bad in these visions, these were heady days. Optimists thought that the Internet's unquenchable communicative freedoms would change the world—make it freer, more efficient, more just, and more democratic.

Indeed, in the '90s there were people—well at least one person, Patrick Ball of the American Association for the Advancement of Science ("AAAS")—traveling around the world to teach democratic political movements in repressive societies how to use cryptography and the Internet to protect their organizing and communications. In the highest risk cases, the activists would not only be trained on how to encrypt their records, but also on how to store them in encrypted databases located abroad. The people who put information into the databases did not have the codes to get it out again; thus, membership lists were safe even from so-called "rubber hose cryptoanalysis."[34]

But not everyone saw the effects of this new technology as benign; some saw the prophesied erosion of state power as an invitation to anarchy, or as opening the door to the very evils that the state power was being deployed to prevent. And even some who might have weighed the overall balance as positive

---

30. This phrase, ubiquitous in the open-information movement, is most often attributed to Stewart Brand, author and founder of The Whole Earth Society. R. Polk Wagner, *Information Wants to Be Free: Intellectual Property and the Mythologies of Control*, 103 COLUM. L. REV. 995, 999 n.14 (2003).

31. Stewart Brand's quote ends with a less well-known sentence: "Information wants to be expensive, because in an Information Age, nothing is so valuable as the right information at the right time." Walter Isaacson, *Information Wants to Be Paid For*, ATLANTIC, July–Aug. 2010, at 46, https://www.theatlantic.com/magazine/archive/2010/07/information-wants-to-be-paid-for/308161/.

32. *See* A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, *in* BORDERS IN CYBERSPACE (Brian Kahin & Charles Nesson eds., 1997).

33. This started as Tim May's signature line in the Cypherpunk mailing list. See Joseph Reagle, *Internet Quotation Appendix*, BERKMAN KLEIN CTR., http://cyber.law.harvard.edu/archived_content/people/reagle/inet-quotations-19990709.html (last visited Jan 16, 2017).

34. *See, e.g.*, Affidavit of Patrick Ball, ACLU v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997) (No. 96-CV-2475-MHS), http://www.aclu.org/technology-and-liberty/affidavit-patrick-ball-aclu-v-miller.

saw it as their duty to enforce the national rules that cyber-enthusiasts were happily undermining.

B. The Three Elements of the Regulatory Project

In the mid-1990s, the Internet really began to change as a result of multiple stresses. New users, and new types of users—people for whom the Internet was a tool, not a dissertation or a toy, and who, due to their large numbers and disparate backgrounds and goals, were not as easily socialized into the informal norms that had tended to keep things orderly—flooded the Internet. As the number of users grew, so too did the visible potential, and then the dollar value, of e-commerce. And a number of more proactive governments began to get excited about existing and imagined capabilities of this growing tide of internet users.

In the United States, the first wave of internet law and regulation had three separate impulses, each a differently motivated reaction to the disruptive effects of a constellation of new technologies based on the communicative power of a network:

1) *Categorization*. The first instinct was to find an existing category in which to pigeonhole the Internet, or, if the Internet could not be categorized, to find categories to which it could be analogized.

2) *New categories* and *new institutions*—ICANN.[35] When existing categories seemed inadequate, the absence of proper pigeonholes created a demand for new ones. When new technology promised new capabilities or new solutions to old problems, these opportunities created a demand for new institutions to enable them. Sometimes, proponents saw in the Internet an opportunity to achieve otherwise unjustifiable regulatory goals. Occasionally enthusiasts enabled solutions that had yet to find problems—e.g., digital-signature regulation.[36]

---

35. For information on the Internet Corporation for Assigned Names and Numbers ("ICANN"), see generally A. Michael Froomkin, *Wrong Turn in Cyberspace*: *Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17 (2000).

36. *Compare* Jane K. Winn, *The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce*, 37 IDAHO L. REV. 353 (2001) (justified skepticism), *with* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 ORE. L. REV. 49 (1996) (early enthusiasm). Note, though, that in the end, digital signatures did become an important internet-security technology. *See* Craig Le Clair et al., *Brief: E-Signature Transactions Topped 210 Million In 2014*, FORRESTER (May 19, 2015), https://www.forrester.com/report/Brief+ESignature+Transactions+Topped+210+Million+In+2014/-/E-RES122671; *Digital Signature Market by Solution, by Services, by Deployment, by Application, and by Region – Global Forecast to 2020*, PR NEWSWIRE (June 8, 2016, 16:21), http://www.prnewswire.com/news-releases/digital-signature-market-by-solution-by-services-by-deployment-by-application-and-by-region---global-forecast-to-2020-300281926.html (forecasting global digital signature market to grow from $512.5 million in 2015 to $2.02 billion by 2020).

3) *Preserving (or reinstating) the status quo*. As government attempts to set technical standards failed—e.g., the Clipper Chip[37]—policymakers legislated more directly—e.g., the United States' Digital Millennium Copyright Act ("DMCA"),[38] the Communications Assistance for Law Enforcement Act ("CALEA"),[39] and the United Kingdom's Regulation of Investigatory Powers Act.[40]

1. Categorization

The legal instinct for categorization came first, both logically and, in time, often to solve disputes: Was the Internet like a telephone network? Or was it more like television? Was computer-mediated speech more like a radio broadcast, a newspaper, or a telephone call?[41] Was e-commerce like mail-order commerce? Is encryption more like speech or a widget?[42] Where does an online transaction occur for jurisdictional purposes? Of course, as in any such exercise, which category an internet-enabled activity would be placed in was often contestable, because there was debate about the true nature of the internet-mediated activity, because analogies are imperfect, because parties dueled about the appropriate level of generality, or because category choice could determine outcomes.

The power of this approach depended on picking the right categories, and sometimes that required recognizing that the old categories were still good ones. We see this perhaps most clearly in the mid- and late-1990s decisions about personal jurisdiction based on web pages. In these cases, some courts tried to fashion a bright-line active/passive site test[43] rather than simply—or perhaps not so simply but still more soundly—trying to apply the principles deriving from personal jurisdiction standards such as *International Shoe*[44] and *Asahi*[45] on a case-by-case basis based on purposeful availment, or conduct directed at a forum, as

37. *See generally* Froomkin, *supra* note 4 (discussing the Clipper Chip).

38. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified at 17 U.S.C. §§ 1201–1205 (2012)).

39. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010 (2012)).

40. Regulation of Investigatory Powers Act 2000, c. 23 (Eng.) ("RIPA"). For a critique of RIPA, see generally Bela Bonita Chatterjee, *New but Not Improved: A Critical Examination of Revisions to the Regulation of Investigatory Powers Act 2000 Encryption Provisions*, 19 INT'L J.L. & INFO. TECH. 264 (2011).

41. This was, in essence, the question the U.S. Supreme Court faced in *Reno v. ACLU*. 521 U.S. 844 (1997). In *Reno*, the Court decided that internet speech was more like a telephone call. *Id.* at 869–70, 75–76 (citing Sable Comms. v. F.C.C., 492 U.S. 115, 129 (1997)).

42. For arguments that encryption is more like speech, see Bernstein v. United States, 176 F.3d 1132, 1135–47 (9th Cir. 1999) (Fletcher, J.), *rehr'g en banc granted*, 192 F.3d 1308 (1999).

43. *See* Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1977) (holding that the greater the commercial nature and level of interactivity of the website, the more likely it is that the website operator will be subject to the forum state's jurisdiction).

44. Int'l Shoe Co. v. Washington, 326 U.S. 310 (1945).

45. Asahi Metal Indus. v. Superior Court, 480 U.S. 102 (1987).

one does in other circumstances.[46] The balance is starting to be restored, but it is taking time.[47]

2. New Categories and New Institutions

A second type of first-wave regulation, usually legislative, sought to create new categories and, in rare cases, new institutions. Sometimes this was because the existing categories seemed inadequate; other times it was because the existence of a new technology promised new capabilities, or new solutions to old problems, or an opportunity to use the Internet as an excuse to achieve a regulatory goal that could not otherwise be justified.

Some cases of this impulse to create new categories went a bit wrong; for example, when the then-rare breed of lawyer-technologists toiled to enable solutions that had not yet found their problems.

The best example of this phenomenon is the Utah Digital Signature Act of 1995,[48] the first of its kind in the nation, and in many ways the model for the ABA guidelines that followed. The Utah law attempted to shape the future by defining transactional roles, rights, and responsibilities in a way that relied on particular technologies used in digital identification and authentication.[49] Those technologies did not catch on in the marketplace nearly as quickly as the law's backers had hoped, nor did the law succeed in kick-starting a new e-commerce industry based on new intermediaries. The Utah model failed more than it succeeded.[50] By contrast, digital signature laws that took a more modest and technology-neutral approach and sought primarily to domesticate deployed technologies and fit them into known categories worked well. It helped to have legislation making clear when an electronic or digital signature counted as a valid signature and when it did not—avoiding many needless court cases.[51] By the late '90s, digital-signature legislation (mostly light-weight) existed in 49 U.S. states, and in many countries.[52]

---

46. *See, e.g.*, Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345 (2001) (critiquing the *Zippo* test and arguing for targeting-based analysis); Joel R. Reindenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951 (2005) (critiquing internet exceptionalism as applied to jurisdiction and arguing for "supremacy of law over technological determinism").

47. For a transnational survey, see generally Christopher Kuner, *Data Protection Law And International Jurisdiction on the Internet*, 18 INT'L J.L. & INFO. TECH. 227 (2010).

48. UTAH CODE ANN. §§ 46-3-101 to 46-3-504 (West 2005) (repealed 2006).

49. *See* Winn, *supra* note 38, at 379 (explaining that laws like the Utah Digital Signature Act are not technology neutral).

50. And in retrospect, it deserved to fail. It turns out there are some serious flaws in the certificate authority infrastructure we have now. *See, e.g.*, Dan Wallach, *Building a Better CA Infrastructure*, FREEDOM TO TINKER (Mar. 30, 2011), http://www.freedom-to-tinker.com/blog/dwallach/building-better-ca-infrastructure. The Utah framework shared these flaws. *See* R. Jason Richards, *The Utah Digital Signature Act as "Model" Legislation: A Critical Analysis*, 17 J. MARSHALL J. COMPUTER & INFO. L. 873, 885–907 (1999) (discussing the various flaws with Utah's approach).

51. The most common approach is that electronic or digital signatures are valid for most things other than wills or conveyances of real property. *See Electronic Signature*

3. Preserving (or Reinstating) the Status Quo

A third set of legal and governmental responses unashamedly sought to return matters to the status quo, or were designed proactively to protect either business models or established governmental practices from internet threats. On occasion, this impulse created something liberty enhancing, such as the European Union's Data Privacy Directive,[53] (although the directive had its roots in the 1980 Organization for Economic Cooperation and Development Guidelines,[54] so perhaps the Data Privacy Directive could be called an especially far-reaching form of categorization). But the most common mainsprings of this impulse were content industries that sought to prevent digital file sharing they saw as destroying their markets and governments concerned by diverse forms of private information exchange—including sedition, conspiracy, libel, threats, and anonymous digital cash—they believed threatened domestic peace and security.

It is important to note that even from an early date, the U.S. government was not the only one concerned by excess communicative freedom. For example, the Canadian government unsuccessfully sought to block U.S. sources from sending daily internet accounts of ongoing Canadian trials—banned domestically on the grounds that these accounts prejudice the defendant's right to a fair trial.[55] At some point, more despotic regimes also began to take note of the Internet's potential and wonder what they should do in response.

But it was the U.S. government—driven, it is widely believed, by the National Security Agency ("NSA"), the people in charge of capturing and analyzing signals intelligence from around the world—who more than anyone first sounded the alarm that widespread untraceable communicative freedom might make their lives more difficult. Similarly, U.S. domestic law-enforcement agencies that relied on wiretaps to make and break cases faced the threat that if all communications were encrypted end-to-end, one of their most valuable law enforcement tools would go the way of the Dodo.[56] It did not help that some Cypherpunks had described a model for a "BlackNet,"[57] a perhaps-real, perhaps-fanciful method for parties to contract, for licit or illicit purposes, without revealing their identity to each other or a third party—the philosophical, but perhaps not in fact genetic, ancestor of WikiLeaks and its ilk—by which

---

Legislation, FINDLAW, http://library.findlaw.com/1999/Jan/1/241481.html (last visited January 16, 2017).

52. The United Nations Commission on International Trade Law (UNCITRAL) adopted lightweight rules for recognition of electronic signatures and legal recognition of data messages in 1996. UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE (1996) (UNITED NATIONS, amended 1998). For example, information shall not be denied legal effect, validity or enforceability solely because it is a data message. *Id.* ch. II, art. 5.

53. EU Data Directive, *supra* note 8, at 31.

54. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last visited Jan. 16, 2017).

55. *See* Froomkin, *supra* note 32, at 146–47 (discussing Canada's attempts to censor reporting of the Karla Homolka criminal case).

56. *See* Froomkin, *supra* note 4, at 744.

57. *See* RID, *supra* note 29, at 278–81.

anonymous leakers could sell their secrets to anonymous buyers and both sides could be assured that their identities would remain unknown to all parties concerned including any intermediaries.[58] "BlackNet" was, its inventor later claimed, just a concept, one designed as an online provocation *pour épater les bourgeois*,[59] but cryptographically powered anonymous remailers were real, and (when they were working properly) they allowed people to send untraceable messages, be they love notes or ransom notes.[60]

Simply banning strong crypto did not seem to be a viable option. There was no statutory authority, and there was no political consensus for new legislation. Worse, there was a First Amendment case—unproven, perhaps, but fervently pushed by its adherents and potentially potent—that such a ban would be unconstitutional.[61] The U.S. government's response was ingenious. Rather than seek new legal powers, the government decided to leverage export-control power it already had, and use that power to set technical standards in a way that would preserve the parts of the status quo it most valued. [62]

The government already prohibited the export of strong cryptography by categorizing it as a dual-use good—a thing that could be used for military as well as civilian purposes. The United States prohibited the export of cryptographic software in the same way. In the mid-'90s, even more than now, the major consumer software companies were based in the United States. Consumer-grade software did not include strong encryption, or in most cases any encryption. One reason was uncertainty about the demand, but the other significant reason was export control: while it was legal to sell encryption to consumers in the United States, it was a major crime to sell it abroad without a license, and those were expensive and time-consuming to obtain. Software companies were very concerned about speed getting to market, and about version control. They did not want to wait around for licenses—even more so if obtaining a license was not a sure thing. Moreover, software companies also did not want to have to make a 'lite' version for export as that would depress foreign sales and require them to maintain and update two versions of their product. Plus, crypto is difficult to implement. Subtle mistakes can destroy a product's security.

The U.S. government's clever ploy was to offer firms the use of an NSA-approved strong cryptographic algorithm, with one little extra: the Clipper Chip. The Clipper Chip would come with an extra method for decrypting messages

---

58. *See* I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993, 1055 (1994) (discussing BlackNet).

59. *See, e.g.*, Tim May, *Untraceable Digital Cash, Information Markets, and BlackNet*, http://osaka.law.miami.edu/~froomkin/articles/tcmay.htm (last visited Jan. 16, 2017).

60. *See* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 U. PITT. J.L. & COM. 395, 414–21 (1996).

61. *See* Bernstein v. United States, 176 F.3d 1132, 1144–45 (9th Cir. 1999) (Fletcher, J.), *rehr'g en banc granted*, 192 F.3d 1308 (1999).

62. *See* Froomkin, *supra* note 4, at 764–76, 793–96; A. Michael Froomkin, *It Came from Planet Clipper: The Battle Over Cryptographic Key "Escrow"*, 1996 U. CHI. LEGAL F. 15, 21–26, 31–33 [hereinafter *Planet Clipper*].

known only to the U.S. government, which it would promise to use only according to specified legal procedures. Win-win, said the government: strong crypto for everyone and we preserve our law enforcement and spy capabilities. In an effort to set a de facto technical standard, the United States started to use the Pentagon's buying power to acquire compliant smart cards, in the hope of creating economies of scale for Clipper-enabled devices and thus setting a market standard too. An important feature of this plan was that every private action—making the chips, selling the chips, and using the devices—could be characterized as formally "voluntary," thus evading or at least burying any constitutional questions.[63]

It almost worked, but instead failed, largely because of a determined effort by privacy activists who raised legal and technical questions about the plan.[64] Governments learned from these failures. Indeed, there is a risk that in time we may come to see them as having lost the battle but won the war because they learned—all too well—from their early failures.

One solution was simply to legislate smarter and more directly. The search for more effective legislation to fight disruptions to settled expectations led governments, even at an early stage, to experiment with choke-point regulation, a development that would come to its full fruition later.[65] If the end-users in democracies were too difficult to police, then the intermediaries on whom they depended for services—Internet Service Providers ("ISPs"), credit-card companies, domain-name registrars, makers of computer and telephone hardware and even software—were far less numerous, easier to find, and far easier to persuade to comply with rules that end-users, given a choice, might well have balked at. The lesson was not lost on regulators in both democracies and despotisms. Where once a government might have sought to set a technical standard or influence the marketplace, now it would legislate it. If code was not law enough, then bring on the law to determine the code— or even the hardware.

An early example of this type of legislation—and of its dangers—was the United States' Communications Assistance for Law Enforcement Act (CALEA) in 1994.[66] The government pitched CALEA to lawmakers as a way to preserve—preserve, not expand—law enforcement wiretapping capabilities by requiring telephone companies to design their networks to be wiretap ready. Since 1994, however, the FBI has used CALEA to expand its capabilities, turning wireless phones into tracking devices, requiring phone companies to collect specific signaling information for the convenience of the government, and allowing interception of packet communications without privacy protections. In 2005, the FCC granted an FBI petition and expanded CALEA to broadband internet access

63. Froomkin, *supra* note 4, at 772–76, 793–96.

64. *Planet Clipper*, *supra* note 62, at 37–45, 67.

65. For an early discussion of choke-point regulation, see generally Peter Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991 (1998).

66. *See* 47 U.S.C. §§ 1001–1010 (2012).

and Voice Over Internet Protocol ("VoIP") services,[67] a decision upheld by the D.C. Circuit in 2006.[68]

The U.S. government deployed a similar choke-point strategy against "cybersquatters," the name coined to describe people who register domain names that share identical character strings with trademarks, and which a small group of profiteers snapped up and then attempted to ransom to brand managers late to the Internet. There, the choke point was the domain-name system, and the central databases run by registries provided easy leverage. The cybersquatter problem was worldwide, and the solution was not just domestic U.S. legislation,[69] but the creation in 1998 of a new formally private body, ICANN, to take over regulation of domain names. With the U.S. government's approval, ICANN's first policy was to create a lightweight arbitration-like system to adjudicate domain-name disputes, one that ended up righting some wrongs, and creating some new ones—in both cases to the advantage of trademark holders, often large firms, some of whom were able to secure victories they could never have won in court, and for only a fraction of the cost.

Three things about ICANN stand out from a legal perspective. First, its scope was international, extending far beyond where any single country's domestic legislation might reach. Second, it was formally a private nonprofit California corporation subject to U.S. law, but in practice it had almost no accountability to anyone other than those it contracted with: as a corporation it was outside public law, and as a self-perpetuating entity with no members, it had the best of private law on its side. Third, the regulations that it imposed on domain name registrants—notably, that they had to agree that their domain names could be taken away if ICANN's arbitration-like process so determined—were an important objective of the U.S. Department of Commerce, which settled on ICANN as the domain-name manager. But because a domain name is acquired by contract between a front-end registrant and a private company that is two private contracts away from ICANN (and thus three from the U.S. government), due process had no traction. Enlisting private parties as de facto regulators proved to be effective.

A larger battle, also with a less-than-happy outcome, raged over file sharing and copyrights. The copyright industry achieved an early victory by securing passage of the DMCA in 1998. DMCA §1201 created what has come be known as a "paracopyright"[70]—legal protection for copy-protection technologies used by copyright holders. This goes beyond traditional copyright in that it not

---

67. *See CALEA Background*, CDT (Sept. 28, 2010), https://www.cdt.org/report/calea-background.

68. Am. Council on Educ. v. FCC, 451 F.3d 226 (D.C. Cir. 2006) (upholding an FCC regulation extending CALEA to VoIP).

69. Anticybersquatting Consumer Protection Act (ACPA), 15 U.S.C. § 1125(d) (2012) (enacted 1999).

70. *See* Peter Jaszi, Address at the Nordiskt Forum for Bibliotekschaefer in Stockholm: Is This the End of Copyright as We Know It? (Oct. 9, 1997) (explaining that the term "paracopyright" refers to new legal protections existing outside of copyright law that were created for copyright owners to enforce against content users who violate the anti-circumvention devices used by copyright owners to secure their material in the online environment).

only prohibits copying of the work and circumventing copy-protection software, but also prohibits the creation or trafficking of tools designed to circumvent copy-protection software. Indeed, §1201 applies regardless of whether the copy-protection technology is effective or not.

Equally important, the DMCA created a method—the takedown notice—by which an allegation of copyright violation would suffice in most cases to force ISPs to immediately take content offline—no injunction needed.[71] That provision and regular copyright law sufficed to enable the killing of file-sharing giant Napster (which was far from an innocent victim). In no time, however, other less centralized music-sharing systems sprang up to replace it.

Thus, by the turn of the century, the U.S. government had learned a great deal about how not to regulate the Internet. With its first taste of choke-point regulation, the government demonstrated that it could control end-users in ways that would have been difficult to impossible to achieve using direct methods. Similarly, in the Clipper Chip debacle, the government learned that it could only leverage technologies into policies if those attempts were not too visible to the users. The Clipper Chip was a tangible thing, both a reminder of the government's role and a target for opposition. Better to go inside existing technologies, or like with CALEA, have the surveillance built into parts of the network where users could not see them. For anonymity, worse was yet to come.

II. THE SECOND WAVE OF INTERNET REGULATION

By 2000, the first wave of internet enthusiasm had already crested. The early heady days of people making use of new technologies and routing happily around legal rules were almost a subject for nostalgia. Even if internet exceptionalism was still alive, in important ways the unregulated Internet had already been subjected to—often ham-handed—attempts to regulate. The Empire—Law's Empire—had struck back.

But this was only the beginning. Governments and industry learned from both their successes and failures, which shaped a second wave of internet regulation. While there are aspects of the second wave that are encouraging, there are even more that are troubling. For instance, it is surely good that internet regulation is increasingly based on a sound understanding of the technology, thereby minimizing needless or unworkable rules. But as regulatory strategies become more effective, there are collateral consequences.

The most significant of those collateral consequences is that the liberty-enhancing aspects of the Internet are now being stifled: where every communication may be recorded, analyzed, cross-referenced, and stored, that which was once clearly liberating is now much more mixed and sometimes quite dangerous to liberty. Where a decade ago it was still reasonable to see the

71. Section 512(c) of the DMCA contains "notice and takedown" provisions, providing that an ISP cannot be liable until it has been put on notice of the alleged infringement. 17 U.S.C. § 512(c) (2012). Once on notice, if the ISP "responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity" it will not be liable. *Id.* To be eligible for invoking the safe-harbor protections, an ISP must meet the conditions set forth under § 512(i).

constellation of technologies around the Internet as fundamentally empowering and anti-totalitarian, that optimism is increasingly difficult to sustain as regulators in both democratic and totalitarian states have learned how to structure rules that cannot easily be evaded, and—increasingly—how to use internet-based technologies to achieve levels of regulatory control that would not have been possible previously.

The examples that follow illustrate four distinguishing characteristics of the second wave of internet regulation: (1) they are based on a much firmer understanding of the underlying technology; (2) they are targeted to use relatively small technological opportunities (choke-point regulation) or require small technological changes (data retention) to achieve large regulatory goals; (3) they are increasingly transnational in character; and (4) they are garnering a growing amount of complaints and resistance.

A. Private Initiatives

It may seem strange to begin a discussion of the new wave of internet regulation aimed at anonymity with private initiatives. After all, regulation is most commonly treated as a governmental function. There are, however, three reasons why the private initiatives described below play a critical role in the campaign against anonymity.

First, and most importantly, "the infrastructure for maintaining civil freedoms and security online is somewhat different than in the physical world. To a larger degree it is embodied by private economic assets."[72] Partly because the technologies are new, and partly because the technologies and business models are in a rapid state of evolution, private initiatives retain a very significant role in shaping the nature of internet regulation. As described below, governments are learning how to regulate, but their choices are often shaped by, and complementary to, decisions made in the private sector. This is particularly true for choke-point regulation, but as we will see also applies more generally.

Second, during the last decade, major western governments, particularly the United States and the United Kingdom, have committed themselves to an ideology of either privatization or co-regulation, in which government and industry share responsibility for drafting and enforcing regulatory standards.[73]

---

72. Fredrik Erixon & Hosuk Lee-Makiyama, *Digital Authoritarianism: Human Rights, Geopolitics and Commerce* 16 (European Ctr. for Int'l Political Econ., Occasional Paper No. 5/2011, 2011), http://www.ecipe.org/app/uploads/2014/12/digital-authoritarianism-human-rights-geopolitics-and-commerce.pdf.

73. *See* Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 441 (2011); Eva Hupkes, *Regulation, Self-Regulation or Co-Regulation?*, 5 J. BUS. L. 427, 427 (2009); Emmanuelle Mazuyer, *La Responsabilité Sociale de L'entreprise et ses Relations avec le Système Juridique*, 26 CAN. J.L. & SOC'Y 177, 189 (2010) (noting co-regulatory enabling features built into EU accords); Paul M. Secunda, *Regoverning the Workplace: From Self-Regulation to Co-Regulation*, 64 INDUS. & LAB. REL. REV. 203 (2010) (reviewing and critiquing CYNTHIA ESTLUND, REGOVERNING THE WORKPLACE: FROM SELF-REGULATION TO CO-REGULATION (2010)); Philip J. Weiser, *The Future of Internet Regulation*, 43 U.C.

Third, and closely related to the first, even though end-users may have incentives to route around identification regimes, many private suppliers of communication technology and communications services have decided that their interests are best served by requiring their customers to identify themselves. Others, such as hardware vendors, have chosen to supply products that are ready to interoperate with identification regimes; some of these products allow the user to control the identifier, but others do not. Thus, many key private players either have no incentive to challenge government attempts to impose identification regimes, or, in some cases, actively support them and lobby for them.

1. Identification to Prevent File Sharing

In the past decade, content owners have stepped up their efforts to stamp out file sharing. In addition to their legislative successes, they have embraced technological solutions, focusing on choke points created by the technologies that most people use to communicate via the Internet. One target has been ISPs. Another target has been the makers of hardware and software. One early and successful effort was to impose region coding on nearly all commercial DVDs, and on both hardware and software DVD players. By contract, the players must be locked to prevent the playing of DVDs sold far away—the fear being the gray market, a form of competition that is legal for almost all other goods.[74] And the content providers were able to convince Congress to make it an offense to circumvent the otherwise defeasible encryption that enforced the regional divisions.[75]

In the past decade, the targets of regulation by technology have been expanded to limit how other home-theater devices interconnect in order to limit home taping. And, in the Orwellian-named "Trusted Computing" initiative, chip-makers are being encouraged[76] (and might someday be required) to place unique identifiers on computer chips that could be invoked by software to identify the machine, without the user's knowledge or consent.[77] Beginning with Intel's Sandy

---

DAVIS. L. REV. 529 (2009); Timothy S. Wu, *Cyberspace Sovereignty?—The Internet and the International System*, 10 HARV. J.L. & TECH. 647 (1997).

74. *See* Rostam J. Neuwirth, *The Fragmentation of the Global Market: The Case of Digital Versatile Discs (DVDs)*, 27 CARDOZO ARTS & ENT. L.J. 409, 413 (2009) (explaining that the DVD Regional Coding System divides the world into different geographical regions so a movie on a DVD from one region can only be watched on the respective hardware manufactured or distributed and sold in the same region).

75. *Id.*

76. *See* Mark Say, *Cabinet Office Backs Trusted Computing*, GUARDIAN (Oct. 21, 2011), http://www.guardian.co.uk/government-computing-network/2011/oct/21/cyber-security-strategy-trusted-computing (reporting that Owen Pengelly, then-deputy director of policy at the Office for Cyber Security and Information Assurance in the Cabinet Office, was "working with a cyber security team in the Department of Business, Innovation and Skills to work out what incentives the government could provide to encourage the take-up of: trusted computing standards").

77. Microsoft and Intel are leading the Trusted Computing initiative. For example, Microsoft's Palladium is an initiative to build anti-copying technology into the hardware and operating system of a PC. This technology will "control" users and limit the abilities of computers. Chad Woodford, *Trusted Computing or Big Brother? Putting the*

Bridge chips in 2011, the chipmaker has included a unique identifier (they call it the "Intel Insider") just waiting for software—not necessarily under the control of the user—to identify it.[78] The hope was that having this capability would give content providers the courage to stream top-quality movies online because they could encrypt it in a way that only a chip with that unique identifier will be able to decrypt.[79] Of course, every internet-connected device already has a unique Media Access Control ("MAC") number, but it is more feasible to change or mask those than something hardwired on the CPU.[80] How successful this initiative has proved

---

Rights Back in Digital Rights Management, 75 U. COLO. L. REV. 253, 280 (2004); *see also* Ryan Roemer, *Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer*, 2003 UCLA J.L. & TECH. 8 (2003). Security researcher Ross Anderson charges that the "Unified Extensible Firmware Interface" (UEFI), a standard for the PC BIOS, is "Trusted Computing 2.0." Ross Anderson, *Trusted Computing 2.0*, LIGHT BLUE TOUCHPAPER (Sept. 20, 2011), http://www.lightbluetouchpaper.org/2011/09/20/trusted-computing-2-0/. Another commentator notes the commercial value:

> Windows 8 PCs will use the next-generation booting specification known as Unified Extensible Firmware Interface ("UEFI"). In fact, Windows 8 logo devices will be required to use the secure boot portion of the new spec. Secure UEFI is intended to thwart rootkit infections by using PKI authentication before allowing executables or drivers to be loaded onto the device. Problem is, unless the device manufacturer gives a key to the device owner, it can also be used to keep the PC's owner from wiping out the current OS and installing another option, such as Linux.

Julie188, *How Microsoft Can Lock Linux off Windows 8 PCs*, SLASHDOT (Sept 21, 2011), http://linux.slashdot.org/story/11/09/21/062231/How-Microsoft-Can-Lock-Linux-Off-Windows-8-PCs. One can easily imagine how this might have antitrust or competition law implications. Microsoft's response has been to state, via one of its blogs, that while UEFI will be required to be enabled by default in order to qualify for Windows Certification, users will be able to turn it off. Steven Sinofsky, *Protecting the Pre-OS Environment with UEFI*, BUILDING WINDOWS 8 (Sept. 22, 2011) ("For the enthusiast who wants to run older operating systems, the option is there to allow you to make that decision.").

78. *See* Richard Adhikari, *Intel Builds Sandy Bridge with a DRM Tollbooth*, TECHNEWSWORLD (Jan. 4, 2011, 5:00 AM), http://www.technewsworld.com/story/71568.html?wlc=1315966732; *Intel Insider – What Is It? (IS It DRM? And Yes It Delivers Top Quality Movies to Your PC)*, BLOGS@INTEL (Jan 4, 2011), https://blogs.intel.com/blog/intel-insider-what-is-it-is-it-drm-and-yes-it-delivers-top-quality-movies-to-your-pc/.

79. Brooks Barnes, *In This War, Movie Studios are Siding with Your Couch*, N.Y. TIMES (Sept. 25, 2010), http://www.nytimes.com/2010/09/26/business/26steal.html.

80. *See, e.g.*, *How to Change a MAC Address*, TECH-FAQ, http://www.tech-faq.com/how-to-change-a-mac-address.html (last visited Jan. 16, 2017). IPv6, the emerging standard for Internet Protocol numbers, *see* Dan York, *What is IPv6?*, INTERNET SOC'Y (Sept. 23, 2011), http://www.internetsociety.org/deploy360/ipv6/, uses the MAC address as part of a device's unique identifier. This makes tracking easy. In response, RFC 4941, an internet standards document, permitted the use of random substitutes for the MAC address in the device's identifier. *See* T. Narten et al., *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, NETWORK WORKING GROUP, http://www.ietf.org/rfc/rfc4941.txt (last visited Jan. 16, 2017). Modern operating systems, including later versions of Android,

to be is unclear as Netflix, YouTube, and others seem to rely on pure software solutions such as the World Wide Web Consortium's encrypted media extensions[81]—some of which still can be circumvented when users reach the sites via proxies that disguise their location.

2. Identification for Profit

In addition to its role as a tool to allow the policing of bad behavior, identity has market value. Firms, especially those seeking to monetize online social networking, increasingly require that users identify themselves not just to the provider, but also to each other.

Where in the '90s it might have been easy to argue that market forces would sort out the privacy and anti-anonymity policies of firms, perhaps leading firms either to compete to be seen as privacy-friendly or to position themselves along a spectrum of privacy by offering policies that would distinguish them from their competitors, that argument seems less plausible today for reasons that have little to do with privacy itself. The past decade has witnessed a powerful market-driven shift towards closure and centralization in both hardware—e.g., the iPhone—and software—e.g., Facebook and Twitter. It may be easier to see how someone will make money off centralized architectures such as Hulu or even YouTube than off decentralized ones such as Gnutella or Bittorent, but it is also far easier to regulate when there is a large central target.

Facebook is a leading example of this phenomenon. It is wildly popular, and is becoming the center of a constellation of applications that link to or from it, or rely on credentials that Facebook provides.[82] Facebook's popularity makes it, like Twitter, an important platform for social activists. For most of its existence, however, Facebook has pursued policies that require users to identify themselves uniquely.[83] According to Access Now, an NGO whose mission is "digital freedom"[84]:

---

iOS, Windows, MacOS, and some flavors of Linux, use the Privacy Extensions defined in RFC 4941. *See* Andrew McConachie, *Privacy Extensions for IPv6 SLAAC*, INTERNET SOC'Y (Aug. 8, 2014), http://www.internetsociety.org/deploy360/resources/privacy-extensions-for-ipv6-slaac/.

81. *See* Stefan Lederer, *Why YouTube & Netflix Use MPEG-DASH in HTML5*, BITMOVIN (Feb 2, 2015), http://www.dash-player.com/blog/2015/02/the-status-of-mpeg-dash-today-and-why-youtube-and-netflix-use-it-in-html5/.

82. *Link Into Your App*, FACEBOOK, https://developers.facebook.com/products/app-links (last visited Jan. 16, 2017); *see also* Caroline McCarthy, *Amid Unrest, a Hard New Look at Online Anonymity*, CNET (Feb. 22, 2011, 3:33 PM), http://news.cnet.com/8301-13577_3-20034879-36.html; James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1146 (2009) ("Facebook's most technologically interesting feature is its 'Platform,' which developers can use to create 'Applications' that plug seamlessly into the Facebook site.").

83. *Statement of Rights and Responsibilities*, FACEBOOK (Jan. 30, 2015), https://www.facebook.com/legal/terms/update ("You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission."). Note that the late 2015 changes to Facebook's enforcement of the real-name policy focused on preventing errors, and did not change the policy itself. Russel Brandom,

> Facebook should be congratulated and condemned in one go: They've built a revolutionary platform that's catalyzed the political change sweeping the Middle East and beyond, but Facebook has also become a treasure trove of information for dictators, allowing them to identify and track down those who oppose them.[85]

Facebook's policy against pseudonyms meant that a leading Chinese blogger had his pages closed[86]; the policy led one wag to suggest that "the world's secret police want you to join Facebook."[87] It may be worth noting that this issue of social-media rules that require identification is only one part of the story regarding the use of new communication tools in resistance to oppressive regimes. Users of these tools often choose to self-identify and also often post content, especially images, that make it possible for security services to identify not just the poster but other protestors, all of whom must then face consequences.[88] That, however, is the user's choice, if sometimes an unwise one. Systems that make anonymous communication impossible remove that choice; systems that merely make anonymity very difficult mean that either the option will be used by few, or if the entire system is too hard to use it will never have mass appeal.

Facebook is dominant in size, but by no means unique. Many other social networks also require users to use their real names. Google+, Google's unsuccessful attempt to compete with Facebook, also required participants to use "the name your friends, family, or co-workers usually call you," or "the name that you commonly go by in daily life"—a policy subjected to substantial criticism.[89]

Facebook Is Changing the Way It Enforces Its Real Name Policy, VERGE (Dec. 15, 2015, 1:00 PM), http://www.theverge.com/2015/12/15/10215936/facebook-real-name-policy-changes-appeal-process.

84. *See Our Mission*, ACCESSNOW, https://www.accessnow.org/about (last visited Jan. 16, 2017).

85. *Facebook, Unfriend the Dictators!*, LEAKSOURCE, (MAR. 15, 2011, 8:24 AM), https://leaksource.wordpress.com/2011/03/15/facebook-unfriend-the-dictators/.

86. *See* Tania Branigan, *Facebook's 'Real Name' Policy Attacked by Chinese Blogger*, GUARDIAN (March 9, 2011, 4:06 PM), http://www.guardian.co.uk/world/2011/mar/09/chinese-blogger-mark-zuckerberg-dog?mobile-redirect=false (noting that "the writer, born Zhao Jing, has used Michael Anti for more than a decade and says even Chinese friends know him as An Ti").

87. Mick Yates, *Why the World's Secret Police Want You to Join Facebook*, MICK'S LEADERSHIP BLOG (Jan. 2, 2011), http://www.leader-values.com/wordpress/?p=3342.

88. This is the critique raised by Evgeny Morozov among others. *See, e.g.*, Evgeny Morozov, *Think Again: The Internet*, FOREIGN POL'Y (Apr. 26, 2010), http://foreignpolicy.com/2010/04/26/think-again-the-internet/ ("Relying on photos and videos uploaded to Flickr and YouTube by protesters and their Western sympathizers, the secret police now have a large pool of incriminating evidence"); Erixon & Lee-Makiyama, *supra* note 72, at 8 (noting authorities' use of BBS and forums to "seek, identify, and suppress citizen dissent").

89. *See* Kaliya Hamlin, *Google+ and My "Real" Name: Yes, I'm Identity Woman*, IDENTITY WOMAN (July 31, 2011), http://www.identitywoman.net/googlereal-name-identity-woman; Kee Hinckley, *On Pseudonymity, Privacy and Responsibility on Google+*, TECHNOSOCIAL (July 27, 2011, 8:45 PM),

Furthermore, there is much more to identity than one's name. Firms—Google chief among them—seek to monetize user-generated content in a variety of ways that often (although not inevitably) require the identification of the user at least with a persistent token, such as a cookie or something similar, if not their actual name. Thus, for example, business models that rely on serving targeted advertising need to know relevant facts about the target's tastes and habits, and may also want to know what advertisements have already been seen in order to avoid repetition. A "persistent token" may sound innocuous, but if any application that uses the token links to the user's real identity, or even in some cases his geo-location, the token becomes an effective identification technology.[90]

In each of these cases, leading firms in their industry have chosen to require user self-identification as the price of access to their highly desirable network. No government regulation was involved.

More recently, however, in 2016, Intel introduced its "True Key" technology, for both PC and mobile devices. True Key functions as a password manager, requiring users to input a typed password, as well as a facial picture and biometric data, in case they forget their "master password." True Key can also identify users through "trusted devices" linked to an e-mail account.[91] Intel stores the users' password, facial and biometric data in servers located in "secure datacenters" in isolated networks. Communication between True Key applications and servers is encrypted in transit.[92] Intel claims that the system's design ensures that its employees cannot acquire any knowledge of users' passwords and other information they have stored in True Key servers,[93] and thus cannot reveal it even if served with a subpoena. True Key is, however, just a way to store passwords, not a content provider. It facilitates, and to a degree protects, users' interactions with other sites; if anything, it facilitates cooperation with other sites' demands for user authentication.

B. Governments

Governments operate against anonymity in electronic communications in two parallel modes: one covert, one overt. The covert mode consists of the capture and, if needed, decryption of communications, as well as secret technical activities designed to make its communications surveillance cheap and easy. The overt mode

---

http://web.archive.org/web/20110729214418/http://www.marrowbones.com/commons/technosocial/2011/07/on_pseudonymity_privacy_and_re.html.

90. These are collectively known as "local shared objects." *See Local Shared Objects – "Flash Cookies"*, ELEC. PRIVACY INFO. CTR. (July 21, 2005), https://epic.org/privacy/cookies/flash.html.

91. Jonathan Keane, *Intel Security's True Key Wants to Do Away with the Master Password Completely*, DIGITAL TRENDS (Mar. 7, 2016), http://www.digitaltrends.com/computing/intel-security-master-password/.

92. Intel uses pervasive TLS, with HSTS (HTTP Strict Transport System) protecting against unauthorized access to data being transferred when users connect through unsecure networks. *Id.* In addition, True Key applications utilize JSON Web Tokens, instead of HTTP cookies, to transfer authenticated data to and from True Key servers. *Id*.

93. *See* INTEL CORP., TRUE KEY BY INTEL SECURITY 1 (2016), https://b.tkassets.com/shared/TrueKey-SecurityWhitePaper-v2.0-EN.pdf.

consists of rules and incentives designed to make anonymity difficult or impossible.

1. Covert Attacks on Anonymity

It is not news that governments spy on each other, on each other's citizens, and even on their own people. Nevertheless, before 2013, few[94] understood the extent to which the U.S. government seeks to capture all of the world's telephonic and computer-mediated communications, and to make it searchable and identifiable. Edward Snowden, an NSA contractor who worked for Booz Allen Hamilton,[95] provided journalists with 1.7 million internal NSA documents.[96] Among other things, the Snowden leaks revealed:

- A Foreign Intelligence Surveillance Act ("FISA") court order requiring the telecommunications company Verizon to provide the NSA with the metadata for all telephone calls in its system "both within the [United States] and between the [United States] and other countries."[97]
- Evidence that since 2007, the NSA ran a surveillance program called Prism, which tracked online communications by sending FISA requests to major technology companies like Google, Facebook, Microsoft, and Yahoo.[98] Through the Prism program, the NSA collected "emails, video clips, photos, voice and video calls, social networking details, logins and other data."[99]

---

94. That is, few other than groups dismissed as fringe elements such as the Cypherpunks, who predicted exactly this more than a decade ago. *See generally, e.g.*, *The Cyphernomicon*, *supra* note 29; RID *supra* note 29.

95. *Who Holds Security Clearances?*, WASH. POST, http://www.washingtonpost.com/world/who-holds-security-clearances/2013/06/10/983744e4-d232-11e2-a73e-826d299ff459_graphic.html (last visited Jan. 16, 2017).

96. Barton Gellman, *Edward Snowden After Months of NSA Revelations, Says His Mission's Accomplished*, WASH. POST (Dec. 23, 2013), http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html; Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Chris Strohm & Del Quentin Wilber, *Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers*, BLOOMBERG BUSINESS (Jan. 9, 2014), http://www.bloomberg.com/news/articles/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.

97. Greenwald, *supra* note 96.

98. *Edward Snowden: Leaks that Exposed US Spy Programme*, BBC NEWS (Jan. 17, 2014), [hereinafter *US Spy Programme*] http://www.bbc.com/news/world-us-canada-23123964; Leo Kelion, *Q&A: NSA's Prism Internet Surveillance Scheme*, BBC NEWS (June 25, 2013), http://www.bbc.com/news/technology-23027764.

99. *US Spy Programme*, *supra* note 98; Kelion, *supra* note 98.

- Extensive—2,776—FISA court and executive order violations by the NSA.[100]
- Evidence that the NSA "collected almost 200 million text messages a day from across the globe, using them to extract data including location, contact networks and credit card details."[101]
- Documentation of the successful effort by the NSA and the United Kingdom's Government Communications Headquarters to hack into the computer systems of Gemalto, a Dutch company that manufactures Subscriber Identity Module ("SIM") cards, a move which allowed the governments to gain access to SIM-card codes and thus facilitate surveillance of mobile-phone communications.[102]
- The existence of NSA data-collection bases in Brazil and 15 other countries around the world that intercept foreign-satellite transmissions.[103]
- Evidence that the NSA changed its minimization rules to allow warrantless searches of U.S. citizens' email and phone calls based on names or other identifying information.[104]

The United States is not the only government with an intelligence agency involved in widespread surveillance.[105] The Canadian intelligence agency, the Communications Security Establishment ("CSE"), tracks millions of video and document downloads daily.[106] Snowden-provided documents also revealed that the NSA shared and received data from government agencies in many countries,

---

100. Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html.

101. James Ball, *NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep*, GUARDIAN (Jan. 16, 2014), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.

102. *US and UK Accused of Hacking SIM Card Firm to Steal Codes*, BBC NEWS (Feb. 20, 2015), http://www.bbc.com/news/technology-31545050.

103. *US Allies Mexico, Chile and Brazil Seek Spying Answers*, BBC NEWS (July 11, 2013), http://www.bbc.com/news/world-latin-america-23267440.

104. *See* James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls*, GUARDIAN (Aug. 9, 2013), http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls.

105. *US Spy Programme*, *supra* note 98.

106. Amber Hildebrand et al., *CSE Tracks Millions of Downloads Daily: Snowden Documents*, CBC NEWS (Jan. 27, 2015), http://www.cbc.ca/news/canada/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120.

including Australia, Canada, Denmark, France, Germany, Israel, Italy, the Netherlands, Norway, Spain, and the United Kingdom.[107]

In order to make its communications interceptions easier and more effective, the NSA worked to undermine national standards in cryptography. For example, in 2006 an NSA employee persuaded the National Institute of Standards and Technology ("NIST") to use a weak random-number generator in a key-encryption standard.[108] Then the NSA paid RSA Security, one of the industry leading security software companies, $10 million to make that weak standard the default formula in its Bsafe encryption product. The not-very-random numbers had the effect of creating a back door allowing the NSA, and potentially others, to decrypt messages encrypted with Bsafe.[109]

Until the Snowden revelations, it might have been plausible to argue that the NSA's capture and analysis of communications and communications metadata did not as a practical matter substantially undermine general communicative freedom, much less the ability to speak anonymously, of U.S. persons and indeed of most foreigners. The argument as to U.S. persons started with the observation that the NSA was not allowed to operate in the United States, so that only international communications, and perhaps the rare domestic communications with

---

107. *See* Sven Bergman et al., *NSA "Asking for" Specific Exchanges from FRA - Secret Treaty Since 1954*, UPPDRAG GRANSKNING (Dec. 8, 2013), http://www.svt.se/ug/nsafra4; Julian Borger, *GCHQ and European Spy Agencies Worked Together on Mass Surveillance*, GUARDIAN (Nov. 1, 2013), http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden; Justin Cremer, *Denmark is One of the NSA's '9-Eyes'*, COPENHAGEN POST (Nov. 4, 2013), http://cphpost.dk/news/denmark-is-one-of-the-nsas-9-eyes.7611.html; Jacques Follorou, *La France, Précieux Partenaire de L'espionnage de la NSA*, LE MONDE (Nov. 29, 2013), http://www.lemonde.fr/technologies/article/2013/11/29/la-france-precieux-partenaire-de-l-espionnage-de-la-nsa_3522653_651865.html; Glenn Greenwald et al., *NSA Shares Raw Intelligence Including Americans' Data with Israel*, GUARDIAN (Sept. 11, 2013), http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents; Hubert Gude et al., *Mass Data: Transfers from Germany Aid US Surveillance*, DER SPIEGEL (Aug. 5, 2013), http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html; Hildebrandt et al., *supra* note 106; Kjetil Malkenes Hovland, *Norway Reveals It Monitored Phone Data*, WALL ST. J. (Nov. 19, 2013), http://www.wsj.com/news/articles/SB10001424052702303985504579207500439573552; Tim Leslie & Mark Corcoran, *Explained: Australia's Involvement with the NSA, the US Spy Agency at Heart of Global Spy Scandal*, ABC NEWS (Nov. 19, 2013), http://www.abc.net.au/news/2013-11-08/australian-nsa-involvement-explained/5079786; Greg Weston et al., *Snowden Document Shows Canada Set Up Spy Posts for NSA*, CBC NEWS (Dec. 9, 2013), http://www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886.

108. *See Standards Lab Overlooked Spy Agency's Cryptography Back Door*, PHYSICS WORLD (Aug. 5, 2014), http://physicsworld.com/cws/article/news/2014/aug/05/standards-lab-overlooked-spy-agencys-cryptography-back-door-say-scientists.

109. *See* Joseph Menn, *Exclusive: Secret Contract Tied NSA and Security Pioneer*, REUTERS (Dec. 20, 2013), http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220.

foreign counter-espionage targets, would be subject to monitoring. Additionally, even if the NSA acquired information about a given communication, it would be loath to share it with other agencies due to a fear that were the fact of the acquisition to become public it would expose NSA "sources and methods," a disclosure that would be necessary in, for example, any prosecution based on that intelligence.[110] In other words, the fact of the collection and the means used to achieve it were such great secrets that no ordinary usage—for example, no prosecution of any single individual—would justify the risk of their exposure. The related argument as to non-U.S. persons similarly relied on the calculus of the dangers of exposure to get over the fact that non-U.S. persons abroad do not have rights under the U.S. Constitution.

In fact, we now know that the NSA collected many, and perhaps nearly all, domestic communications.[111] And there are numerous reports that the NSA shared the fruits of its data collection with other agencies, including the Drug Enforcement Administration, the Internal Revenue Service,[112] the FBI, and perhaps up to two dozen other agencies.[113]

Worse, unless they lead to legal changes, the Snowden revelations may have a perverse effect on communications privacy. Although it now appears that the NSA was in fact sharing the information that it gathered with certain other agencies, the NSA required the recipient agency to obscure the source of the information via a process it called "parallel construction" (but which critics have called "intelligence laundering").[114] Now that the fact of the NSA's routine collection of domestic communications is public, the NSA's disincentive to share what it learns widely within the government should be significantly reduced, leading to an increase in the use of that information.

Meanwhile, some European governments found ways to circumvent data collection and transfer regulations in order to implement and facilitate identification requirements. For example, the Romanian government has recently been funded by the European Union to acquire and install software and hardware

---

110. Indeed, in *Clapper v. Amnesty Int'l*, the Supreme Court said as much: "If the Government intends to use or disclose information obtained or derived from a § 1881a acquisition in judicial or administrative proceedings, it must provide advance notice of its intent, and the affected person may challenge the lawfulness of the acquisition." 133 S. Ct. 1138, 1154 (2013).

111. *See supra* notes 97–104.

112. John Shiffman & David Ingram, *Exclusive: IRS Manual Detailed DEA's Use of Hidden Intel Evidence*, REUTERS (Aug. 7, 2013), http://www.reuters.com/article/2013/08/07/us-dea-irs-idUSBRE9761AZ20130807.

113. Ryan Gallagher, *The Surveillance Engine: How the NSA Built Its Own Secret Google*, INTERCEPT (Aug. 24, 2014), https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/. *See generally* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD (2015) (describing the vast extent of governmental and corporate surveillance of individuals).

114. *See* Hanni Fakhoury, *DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations*, ELEC. FRONTIER FOUND. (Aug 6, 2013), https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering.

aimed at "consolidating and assuring eGovernment interoperability between public information systems," as part of an initiative called "SII Analytics."[115] Essentially this will result in all public institutions feeding personal, corporate, and tax information into a single system. In accordance with this, all Romanian public entities will have unlimited and unwarranted access to these data sets. The system also includes statistical analysis capabilities, allowing it to cross-reference data fed into the system. Facial recognition capabilities have also been included in the system, in order to prevent fraud. SII Analytics will be able to intercept internet traffic originating in mobile instant messaging applications and other sources.[116] This initiative appears to violate limits set by the European Court of Justice ("ECJ") on how government authorities collect and transfer personal data.[117]

2. Overt Attacks on Anonymity

Governments have become increasingly active in regulating anonymity online, either as an end in itself or as part of a larger package of rules designed to regulate online communication. "Currently, there are now over forty countries involved in physically restricting information flow on the Internet, compared to a handful ten years ago."[118]

The regulatory impulse has many sources, but content-based concerns frequently figure importantly among them. Yaman Akdeniz, writing for the Organization for Security and Co-operation ("OSCE") in Europe, aptly summarizes these governments' agendas:

> Governments are particularly concerned about the availability of terrorist propaganda, racist content, hate speech, sexually explicit content, including child pornography, as well as state secrets and content critical to certain governments or business practices. However, the governance of illegal as well as harmful (which falls short of illegality) Internet content may differ from one country to another and variations are evident within the OSCE participating States. "Harm criteria" remain distinct within different jurisdictions with individual states deciding what is legal and illegal based upon different cultural, moral, religious, and historical differences and constitutional values.[119]

---

115. *Romanian Secret Services Uses European Funding for Mass Surveillance Project Disguised as eGovernment Services*, APTI (Aug. 8, 2016), https://privacy.apti.ro/2016/08/08/romanian-secret-services-uses-european-funding-for-mass-surveillance-project-disguised-as-egovernment-services/.

116. *Romania: Mass Surveillance Project Disguised as eGovernment*, EDRi (Aug. 24, 2016), https://edri.org/romania-mass-surveillance-project-disguised-egovernment/; *Romanian Secret Services Public Statement Confirms Suspicions Regarding Mass Surveillance*, APTI (Aug. 9, 2016), https://privacy.apti.ro/2016/08/09/romanian-secret-services-public-statement-confirms-suspicions-regarding-mass-surveillance/.

117. *See infra* text accompanying note 226–29.

118. Erixon & Lee-Makiyama, *supra* note 72, at 4.

119. Yaman Akdeniz, ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE, REPORT, FREEDOM OF EXPRESSION ON THE INTERNET 4–5 (citation omitted), http://www.osce.org/node/80723.

Any nation seeking to undertake a regulatory project of this nature must take a position on anonymity. It took only a little experience with the Internet for governments to understand its implications for both trans-border and domestic communications.[120] It took only a little longer to understand that if users could remain anonymous, they could continue the communications judged to be harmful with relatively little fear of sanctions. With regards to anonymity, the governmental reaction to this realization had three main components. Governments sought to find points of maximum leverage—choke points—for regulation. Governments brought in rules that required users to identify themselves or required communications intermediaries to do the identifications. And governments brought in data retention rules so that communications intermediaries would preserve data that would make investigations of internet-based offenses—including but not limited to harmful communications—more likely to be fruitful.

In addition, governments learned to cooperate in order to reduce the potential scope of regulatory arbitrage. As we will see, two transnational agreements, the Cybercrime Convention (Council of Europe, 2001), and the Directive on Mandatory Retention of Communications Traffic Data (European Union, 2006) have been significant in either requiring, or at least providing cover for, national rules that place limits on communicative freedom (or, the rules' supporters would say, communicative anarchy). Where in the first wave of regulation the main location of regulation was at the national (or, often, in the case of private law in the United States, sub-national) level, in the second-wave, regulation has a much more transnational dimension, at least as regards issues considered to involve crime or public order or to impact national security. The move to supra-national rulemaking and supra-national institutions was hardly unique; rather, it was part of a larger growth of supranational institutions such as the WTO, the hallmarks of what we now call globalization.

a. Choke-Point Regulations

At first the Internet seemed to be the modern Hydra.[121] Every attempt to stop information from moving across borders seemed destined to fail, as the 'net exploded with new methods for file sharing, new types of encryption, anonymous remailers and the like. The very design of Transmission Control Protocol/Internet Protocol ("TCP/IP"), with its ability to route around censorship and "treat it as damage,"[122] seemed to enthusiasts to impose strict limits on the project of communications regulation.

In fact, however, two existing models demonstrated that properly designed rules could take advantage of aspects of the new technology that created continuing opportunities for determined regulators. The international campaign against money laundering likely served as the most important model for this choke-point regulation. By focusing regulatory energies on banks and other

120. *See supra* Section I.B.

121. *See* Froomkin, *supra* note 32.

122. Philip Elmer-DeWitt, *First Nation in Cyberspace*, TIME (Dec. 6, 1993), http://content.time.com/time/magazine/article/0,9171,979768,00.html (quoting John Gilmore).

financial intermediaries, regulators were able to leverage their control of one highly regulated sector of the economy into a potent form of information gathering about other potentially illicit economic activity, followed by restrictions on that illicit activity. Through devices such as "know your customer" rules and legal requirements to report any substantial cash transaction, banks were recruited, willingly or not, as enforcers. The success of this model was not lost on regulators, who sought ways of translating it to the Internet.

A much smaller-scale version of this process soon was enacted via ICANN. The centralized nature of the domain name system ("DNS") made it a natural choke point for regulation of trademark issues relating to domain names. The U.S. government required ICANN to require all registrars and registries who wished to participate in the legacy root to take part in the administrative system ICANN designed to decide claims of cybersquatting.[123] But in internet terms the DNS was arguably uniquely centralized, and the challenge remained whether the choke-point model could be applied more generally.

It turned out that it could be. In some cases this was simply a matter of using the financial system. For example, in its effort to stamp out off-shore internet-based gambling, the United States passed the Unlawful Internet Gambling Enforcement Act of 2006,[124] empowering U.S. regulators to require credit-card operators to identify and prevent the payment of funds for internet gambling,[125] an authority they duly exercised, effective December 1, 2009.[126] As a result, the job of stopping U.S. credit-card holders from using the cards to gamble was, in effect, outsourced to the credit-card issuers. While it may not have worked perfectly, it was effective enough to encourage a "copycat effect"[127] in which government first drafted financial and then other intermediaries as proxies in its efforts to regulate online activities.

Choke-point regulation seemed likely to be effective against online activities for two other reasons: one technical, and one economic and sociological. The technical reason related to discoveries about the paths that internet communications typically take. While TCP/IP allows for a very decentralized routing system, the reality is that there are, in practice, a small number of information super-highways that carry a disproportionate amount of internet traffic. Thus, for example, "[r]esearchers found in 2009 that the [United States] and [United Kingdom] are the two most 'central' countries carrying international internet traffic."[128] Conversely, some countries rely on a single, or a very small

---

123. *See supra* text accompanying notes 26 and 58; *see also* A. Michael Froomkin, *ICANN's "Uniform Dispute Resolution Policy": Its Causes and (Partial) Cures*, 67 BROOK. L. REV. 605 (2002).

124. Pub. L. No. 109-347, 120 Stat. 1884 (2006) (codified at 31 U.S.C. §§ 5361–5367 (2012)).

125. 31 U.S.C. § 5364 (2012).

126. Prohibition on Funding of Unlawful Internet Gambling, 73 Fed. Reg. 69,382, 69,382 (Nov. 18, 2008) (codified at 31 C.F.R. pt. 132).

127. *See* Mark MacCarthy, *What Payment Intermediaries are Doing About Online Liability and Why It Matters*, 25 BERKELEY TECH. L.J. 1037, 1070–71 (2010).

128. *See* Ian Brown, *Communications Data Retention in an Evolving Internet*, 19 INT'L J.L. & INFO. TECH. 95, 102 (2010).

number, of internet cables for the international internet access, creating a single point of failure[129]—or a single target for regulation, such as the notorious "Great Firewall of China."[130]

Of potentially even greater significance, however, is the network effect that drives the economics of important internet intermediaries in both search engines and social media. If, as it appears, network effects frequently predominate in the internet economy,[131] then the competition be the most popular search engine, virtual world, or social-media platform tends to produce winners, dominant players who themselves then can become targets for choke-point regulation.

b. Identification Requirements

Even countries that do not seek to restrict local information flow nonetheless desire the ability to monitor communications for law enforcement and national security reasons. Increased concern with hackers and cyberwarfare only intensifies the desire to be able to identify the source of any potentially dangerous or intrusive packet of computer information. While the degree of intrusion and the willingness to enforce aggressively against end-users as opposed to only targeting intermediaries varies substantially, a push towards identification requirements can be found both in democratic and nondemocratic nations, and at both the national and international level.

The sharpening of national policy was already clear early in the last decade. On November 23, 2001, 30 countries, including the United States and the members of the European Union, signed the Council of Europe Convention on Cybercrime[132] ("the Cybercrime Convention"). The agreement, which was open to accession by nonmember states of the Council of Europe, requires parties to establish laws against cybercrime, to provide authority for domestic law enforcement to investigate and prosecute computer-related offenses, and to provide international cooperation to other parties in the fight against computer-related crime.

---

129. *See* Laurence Reza Wrathall, *The Vulnerability of Subsea Infrastructure to Underwater Attack: Legal Shortcomings and the Way Forward*, 12 SAN DIEGO INT'L L.J. 223, 252 (2010).

130. *See, e.g.*, Jonathan Zittrain & Benjamin Edelman, *Empirical Analysis of Internet Filtering in China*, BERKMAN CTR. INTERNET & SOC'Y (Mar. 20, 2003) http://cyber.law.harvard.edu/filtering/china/. For a more holistic view of the Chinese approach to controlling the internet, see Rogier Creemers, *The Privilege of Speech and New Media: Conceptualizing China's Communications Law in the Internet Era*, *in* THE INTERNET, SOCIAL MEDIA AND A CHANGING CHINA (Jacques DeLisle, Avery Goldstein, & Guobin Yang eds., 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2379959.

131. *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS (2006), http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf (arguing that networked economy enables new, more valuable methods of social production).

132. Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 [hereinafter Convention on Cybercrime], http://conventions.coe.int/Treaty/en/cadreprincipal.htm. For a list of signatories, including dates of signature, ratification, and entry into force, see *Chart of Signatures and Ratifications of Treaty 185*, COUNCIL EUR., http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG (last visited Feb. 27, 2017).

The Cybercrime Convention was and remains controversial. Its supporters characterize it as a relatively innocuous agreement designed to promote a basic level of standardization among national legal regimes and to provide a legal foundation for transnational cooperation between law enforcement and prosecutors.[133] Critics painted it as a back door to legal process that could allow foreign governments to demand domestic assistance in spying on expatriate dissidents, lacking in privacy protections and judicial review.[134] In particular, they pointed to Article 14, which they read to require countries to enact legislation compelling individuals to disclose their decryption keys in order to allow for law-enforcement access to computer data.[135] An additional optional protocol required states to criminalize online racist and xenophobic speech,[136] a requirement attacked as infringing rights of free expression. Regardless of which side more accurately characterized what the Convention requires, a number of national governments have used accession and ratification of the Convention as grounds for enacting legislation that requires data retention or requires communication intermediaries to collect and retain identification information about their customers.

The last decade has seen a very significant expansion of identification requirements as a precondition to the use of modern communications. Identification requirements span a number of information technologies, touching cell phones, computer hardware, computer software, and especially communications service providers, such as ISPs.

Many countries, including a number of democracies, have adopted rules requiring sellers of mobile phones and other devices to collect and identify prepaid

---

133. *E.g.*, U.S. Dep't of Justice, *Frequently Asked Questions and Answers: Council of Europe Convention on Cybercrime (update as of November 10, 2003)*, WAYBACK MACH., [http://web.archive.org/web/20060222055146/http://www.cybercrime.gov/COEFAQs.htm#QA4] (last visited Feb. 10, 2017) (touting the value of convention in fighting the rapidly growing threat of cybercrime); *see also* Declan McCullagh & Anne Broache, *Senate Ratifies Controversial Cybercrime Treaty*, CNET (August 4, 2006, 4:46 AM), http://news.cnet.com/2100-7348_3-6102354.html (quoting Sen. Richard Lugar as saying Convention "will enhance our ability to cooperate with foreign governments in fighting terrorism, computer hacking, money laundering and child pornography, among other crimes").

134. *See, e.g.*, Letter from Marc Rotenberg, President, EPIC, to Senator Richard G. Lugar, Chairman, and Joseph R. Biden Jr., Ranking Member, Senate Comm. on Foreign Relations (July 26, 2005), http://www.epic.org/privacy/intl/senateletter-072605.pdf.

135. Article 14 requires that participating countries enact legislation empowering law-enforcement authorities "to order for the purposes of criminal investigations or proceedings any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide all necessary information, as is reasonable, to enable the undertaking" of the seizure of such data. Convention on Cybercrime, *supra* note 132, art. 14.

136. Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, Jan. 28, 2003, E.T.S. No. 189, http://conventions.coe.int/Treaty/en/Treaties/html/189.htm.

mobile users' contact information for later potential use by law enforcement.[137] Switzerland, for example, was an early adopter, requiring buyers to show IDs or passports to permit the registration of prepaid SIM cards as early as 2003 in response to news reports that Al Qaeda was purchasing unregistered phones.[138]

Mexico's more recent rule imposes a considerably more extreme identification requirement. To obtain a mobile-phone number in Mexico, citizens are required to provide proof of their current address, present the unique identity code given to both citizens and residents of Mexico, produce valid photo identification, and submit to fingerprint scanning. In accordance with the law, Mexican mobile-phone companies are responsible for encouraging the users of their 80m devices to register with the National Registry of Mobile Phone Users.[139]

Many countries now require ID to use public internet facilities, such as those in internet cafes, including Brazil, China, India, Japan, and Peru.[140] The Brazilian government fined Google for refusing to reveal the identities of anonymous bloggers who accused a small-town mayor of corruption and embezzlement.[141] And, until the courts struck it down, at least one American locality wanted to not just require ID, but also monitor what content users accessed in a cybercafe.[142]

Text messaging has been a significant target of governments around the world. Research In Motion ("RIM"), the makers of BlackBerry smart phones,

---

137. *See* Katitza Rodriguez, *The Politics of Surveillance: The Erosion of Privacy in Latin America*, POGOWASRIGHT.ORG (July 27, 2011), http://www.pogowasright.org/?p=23846 (Peru, Brazil, and Mexico).

138. Jonh Lettice, *Swiss Move to Block Al Qaeda Mobile Phone Supply*, REGISTER (Mar. 12, 2003, 17:03), http://www.theregister.co.uk/2003/03/12/swiss_move_to_block_al/.

139. Rodriguez, *supra* note 137.

140. *See* Kuchikomi, *New ID requirements for Net cafes unlikely to deter cyber-crimes*, JAPAN TODAY (July 21, 2010, 6:02 AM), http://www.japantoday.com/category/kuchikomi/view/new-id-requirements-for-net-cafes-unlikely-to-deter-cyber-crimes (explaining that Japanese customers must provide the cybercafe with their identification cards); Jane Macartney, *China Photographs All Internet Café Customers*, AUSTRALIAN (Oct. 17, 2008, 12:00 AM), http://www.theaustralian.com.au/news/china-photographs-all-web-cafe-users/story-e6frg6t6-1111117779729; Arun Prabhudesai, *New Cyber Café Rules in India*, TRAK-IN INDIA BUSINESS BLOG (Apr. 26, 2011), http://trak.in/tags/business/2011/04/26/cyber-cafe-rules-india-guidelines/ (Indian customers must provide the cyber-café with identification and agree to have their picture taken); Rodriguez, *supra* note 137.

141. The fine was about $141,000 U.S. Dollars. *See* Anna Heim, *Google Fined in Brazil for Refusing to Reveal Bloggers' Identities*, TnW (Aug. 20, 2011), http://thenextweb.com/la/2011/08/20/google-fined-in-brazil-for-refusing-to-reveal-bloggers-identities/?awesm=tnw.to_1ASTX&utm_campaign=&utm_medium=tnw.toother&utm_source=t.co&utm_content=spreadus_master.

142. *See* Vo v. City of Garden Grove, 115 Cal. App. 4th 425, 447 (2004) (striking down ordinance requiring cybercafes to install video system that must be "capable of delineating on playback . . . the activity and physical features of persons or areas within the premises," and that "cover all entrances and exit points and all interior spaces, excepting bathroom and private office areas" whose tapes "shall be maintained for a minimum period of 72 hours").

found itself struggling with several countries, including India and the United Arab Emirates. These countries demanded that the company hand over the keys to the encrypted messages sent by BlackBerry users.[143] Although it initially opposed efforts by the Indian government to monitor BlackBerry message traffic, by 2011 RIM had capitulated and was reported to have aided Indian authorities in setting up a domestic monitoring facility.[144] Similarly, several years ago, Pakistan became concerned about end-to-end encryption of mobile telecommunications, wanting calls in clear at each base station so that they could be easily wiretapped.[145] The Pakistani government has now added a ban on encryption of email and of Virtual Private Networks ("VPNs")[146] to the regulation of telecom encryption formally promulgated in the Pakistani Monitoring & Reconciliation of International Telephone Traffic Regulations 2010.[147] The government justified this ban as an anti-terrorism measure, but its effect is to make formerly secure communications, a routine part of much e-banking and e-commerce, no longer possible.[148] Similarly, citing concerns that terrorists might make unmonitored communications, the Indian government proposed a new international standard to the International

143. Troy Wolverton, *Privacy Advocates Criticize Government's Online Eavesdropping Proposal*, SAN JOSE MERCURY NEWS (Sept. 27, 2010), http://www.mercurynews.com/2010/09/27/privacy-advocates-criticize-governments-online-eavesdropping-proposal/.

144. *See* Tom Jowitt, *RIM Establishes Indian BlackBerry Surveillance Lab*, SILICON (October 28, 2011, 7:41 PM), http://www.silicon.co.uk/workspace/rim-establishes-indian-blackberry-surveillance-lab-44065; Amol Sharma, *RIM Facility Helps India in Surveillance Efforts*, WALL ST. J. (Oct. 28, 2011), http://online.wsj.com/article/SB10001424052970204505304577001592335138870.html.

145. "A press report in the Karachi Daily Dawn reported on February 26, 1995, that the government of Pakistan shut down a cellular network run by Mobilink, a joint venture between Motorola and Pakistani SAIF Telecom, because it was unable to intercept traffic." NAT'L RESEARCH COUNCIL, COMPUT. SCI. & TELECOMMS. AUTH., CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 438 (1996).

146. *See* Josh Halliday & Saeed Shah, *Pakistan to Ban Encryption Software*, GUARDIAN (Aug 30, 2011, 14:26), http://www.guardian.co.uk/world/2011/aug/30/pakistan-bans-encryption-software; *Internet Operators in Pakistan Directed to Prevent Private Browsing*, DOMAIN-B.COM (Aug. 29, 2011), http://www.domain-b.com/infotech/itnews/20110829_private_browsing.html ("According to a [Pakistan Telecommunications Authority] spokesman the directive was intended only to stop militants from using secure internet connections to communicate with each other. However, he admitted that this was only possible by preventing all internet users in Pakistan from using virtual private networks ('VPNs'), according to the Express Tribune newspaper."); Mike Masnick, *Reports Claim that Pakistan is Trying to Ban Encryption Under Telco Law*, TECHDIRT (July 29, 2011, 12:28 PM), https://www.techdirt.com/articles/20110729/03142715310/reports-claim-that-pakistan-is-trying-to-ban-encryption-under-telco-law.shtml.

147. *See* Barbora Bukovska, *Statement: Pakistan: Ban on Internet Encryption a Violation of Freedom of Expression*, ARTICLE 19 (Sept. 2, 2011), https://www.article19.org/resources.php/resource/2719/en/pakistan:-ban-on-encrypted-software-a-violation-of-freedom-of-expression (critiquing the 2011 directive implementing the 2010 regulations).

148. *See* Halliday & Shah, *supra* note 146; Masnick, *supra* note 146.

Telecommunication Union that would automatically disable satellite telephones when brought into countries, like India, that ban their use.[149]

The UK government has, for some time, been struggling with the issue of mandatory identification at several levels, not just for information technology. A proposal for a mandatory national ID system, begun under the Labor government,[150] was scrapped by the Conservative-Liberal Democrat coalition government that replaced it in 2010.[151] The government continued to worry about the problem of identity, and sought to appear receptive to proposals such as "Clare's Law"—a campaign sponsored by police chiefs, the Victims Commissioner, and others in the name of a woman murdered by a man she met on Facebook—which would have sought to create a system by which women could check if potential partners had a record of domestic violence.[152] The urban riots of summer 2011 spurred new calls by the UK government, or at least the dominant Tory coalition partner, to explore social-media regulation. The Prime Minister, David Cameron, stated in Parliament that:

> Free flow of information can be used for good. But it can also be used for ill.
>
> And when people are using social media for violence we need to stop them.
>
> So we are working with the Police, the intelligence services and industry to look at whether it would be right to stop people communicating via these websites and services when we know they are plotting violence, disorder and criminality.[153]

These remarks were greeted with glee in China,[154] and with silence in the United States.[155] After public protest, the UK government announced it would not

---

149. Nate Anderson, *India Seeks to Disable Satellite Phones at the Border to Fight Terrorism*, ARS TECHNICA (Sept. 22, 2011, 11:11 AM), http://arstechnica.com/tech-policy/news/2011/09/india-seeks-to-disable-satellite-phones-at-the-border-to-fight-terrorism.ars.

150. *See* UK Identity Cards Act 2006, c. 15 (Eng.) (providing for physical card linked to the National Identity Register database).

151. *See* Identity Documents Act 2010, c. 40 (Eng.) (repealing Identity Cards Act 2006).

152. *See Government Considers 'Clare's Law'*, TELEGRAPH (July 16, 2011, 10:05 PM), http://www.telegraph.co.uk/news/uknews/law-and-order/8643014/Government-considers-Clares-Law.html.

153. Prime Minister David Cameron, Statement Before the House of Commons (Aug. 11, 2011) (transcript available at http://www.number10.gov.uk/news/pm-statement-on-disorder-in-england/); *see also* Uri Friedman, *Twitter Braces for U.K. Censorship Following the Riots*, ATLANTIC (Aug. 22, 2011), http://www.theatlantic.com/international/archive/2011/08/twitter-braces-censorship-following-uk-riots/353987/.

154. *See* Sara Jerome, *Web Freedom Advocates Approve of Clinton's Response to UK Social Media Furor*, NEXTGOV (Aug. 18, 2011), http://www.nextgov.com/nextgov/ng_20110818_1620.php (quoting Andrew McLaughlin, former U.S. deputy chief technology officer, who described the Chinese reaction as "gleeful"); *see also* Ravi Somaiya, *In Britain, a Meeting on Limiting Social Media*, N.Y.

seek additional powers to regulate social media, but would instead seek "voluntary ways to limit or restrict the use of social media to combat crime and periods of civil unrest."[156]

Meanwhile, RIM already had agreed to give British police access to user data from its BlackBerry Messenger network under certain—unspecified—circumstances.[157] During and after the 2011 riots, British authorities identified the encrypted messages sent via BlackBerry Messenger as a prime vector for riot to organization and strategy. A RIM spokesperson stated that the firm would consider automating the process for future access.[158] Earlier, RIM had negotiated with Saudi Arabia and India to allow some monitoring of users' messages.[159]

In the United States, the government has not sought to make anonymity illegal or to require identification directly. Indeed, a legal requirement that persons identify themselves online would not only be controversial but would also likely be unconstitutional.[160] Most internet and cell-phone communications originate from devices that are linked to a user by the service provider; access control and identification are required both for billing purposes and for fear that unidentified persons might hack or otherwise harm the system. Identification is thus something of a default for commercial reasons, and for security reasons even in nonprofit settings.[161] And, unlike the European Union, the United States has not attempted to enact an equivalent to the Data Protection Directive or similar rules to act as a counterweight to the private retention of data. The issue is to what extent users will remain able to use tools to change the default and to mask their identity. On this question, the U.S. government appears to be pursuing contradictory policies, some of which might even enhance anonymous communication, while others seem calculated to make it difficult or impossible.

TIMES (Aug. 25, 2011), https://www.nytimes.com/2011/08/26/world/europe/26social.html (noting that Iran offered to "send a human rights delegation to Britain to study human rights violations in the country").

155. *See* Jerome, *supra* note 154 (noting that the U.S. government, which previously had spoken out against government censorship of social media, chose to say "exactly nothing" about the U.K. trial balloon).

156. Somaiya, *supra* note 154.

157. *Id.*

158. *Id.*

159. *See* ET Bureau, *RIM Gives India Access to Messenger Services*, ECON. TIMES (Jan 14, 2011, 3:05 AM) http://articles.economictimes.indiatimes.com/2011-01-14/news/28430015_1_security-architecture-corporate-email-blackberry-enterprise-server; *Saudi Arabia Halts Plan to Ban BlackBerry Instant Messaging*, TELEGRAPH (Aug. 7, 2010, 11:43 AM) http://www.telegraph.co.uk/technology/blackberry/7931768/Saudi-Arabia-halts-plan-to-ban-BlackBerry-instant-messanging.html.

160. *See infra* text accompanying notes 254–56.

161. One such fear is of spammers using resources to send large numbers of spam messages. These messages can not only strain the network but also cause recipient networks to blacklist the sending organization, thus further interfering with legitimate network traffic. Reeshma Mathews, *Email Blacklist Removal – How to Stay off Blacklists for Uninterrupted Mail Service*, BOBCARES BLOG (Jan. 31, 2017), https://bobcares.com/blog/email-blacklist-removal/.

The Obama Administration's *National Strategy for Trusted Identities in Cyberspace*[162] epitomizes one side of the division. The *Strategy* envisions an "Identity Ecosystem" described as a system that will enhance privacy and civil liberties:

> The Identity Ecosystem will use privacy-enhancing technology and policies to inhibit the ability of service providers to link an individual's transactions, thus ensuring that no one service provider can gain a complete picture of an individual's life in cyberspace. By default, only the minimum necessary information will be shared in a transaction. For example, the Identity Ecosystem will allow a consumer to provide her age during a transaction without also providing her birth date, name, address, or other identifying data.
>
> In addition to privacy protections, the Identity Ecosystem will preserve online anonymity and pseudonymity, including anonymous browsing.[163]

While setting out the outlines of how such a system might work in theory, the Commerce Department's *Strategy* does not attempt to explain key aspects of how its ambitious goals might be attained in practice. Instead, it sets out a ten-year roadmap, in which the first three to five years require "standardization of policy and technology."[164] The key to implementation, we are told, rests on the twin pillars of underlying reliable offline credentials[165] and private-sector leadership.

Ultimately, the Identity Ecosystem can be designed and built only by the private sector. The federal government will support the private sector, ensure that the Identity Ecosystem respects the privacy and otherwise supports the civil liberties of individuals, and be a leader in implementing the Identity Ecosystem in its own services. Existing efforts by the public and private sectors have already established services that are significant components of the Identity Ecosystem, but much remains to be done. Individuals, businesses, nonprofits, advocacy groups, associations, and all levels of government must work in partnership to improve how identities are trusted and used in cyberspace.[166]

Only one month later, however, the Obama Administration released its *International Strategy for Cyberspace*, a document that while extolling the Internet's benefits and opportunities, also warned darkly of its dangers.

Extortion, fraud, identity theft, and child exploitation can threaten users' confidence in online commerce, social networks, and even their personal safety.

---

162. *See* WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE (2011), [http://web.archive.org/web/20170120221811/http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf].

163. *Id.* at 2.

164. *Id.* at 40.

165. *Id.* at 8. The *Strategy* does not explicitly address identity and trust issues in the offline world; however, offline and online identity solutions can and should complement each other. Identity proofing (verifying the identity of an individual) and the quality of identity source documents have a profound impact on establishing trusted digital identities, but the *Strategy* does not prescribe how these processes and documents need to evolve.

166. *Id.* at 42.

The theft of intellectual property threatens national competitiveness and the innovation that drives it. These challenges transcend national borders; low costs of entry to cyberspace and the ability to establish an anonymous virtual presence can also lead to "safe havens" for criminals, with or without a state's knowledge. Cybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace.[167]

Rather than commit to protecting anonymity, this policy document suggested that while privacy was important, the main goals were notice and the active role of government to protect users from evils while subject to "judicial review and oversight."[168] Thus, the Internet of the future should be "secure"—in the sense of not allowing bad actors free reign, rather than in the sense of fostering communications free from third-party monitoring or accountability.[169] Fundamental values of freedom of expression and privacy (defined as "arbitrary or unlawful" state action) would be balanced against "respect for intellectual property rights" and "protection from crime."[170]

And, as described in more detail in the next Section, the Obama Justice Department endorsed, at least in principle, a mandatory data-retention scheme under which ISPs would have to retain customer information, including their IP numbers and times of access, that would allow the identification of most customers most of the time.[171] Meanwhile, spokesmen for the FBI and the U.S. Defense Department issued a series of alarming statements about the dangers of anonymous cyberattacks,[172] and the construction of a "National Cyber Range" to test internet military technologies,[173] although the initial (public) response focused on

---

167. WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 4 (2011), [http://web.archive.org/web/20160516130756/http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf].

168. *Id.* at 5.

169. *See id.* at 8 (defining "Our Goal" as, "an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace").

170. *Id.* at 10.

171. *See infra* text accompanying note 188.

172. *See, e.g.*, Michael Riley et al., *Anonymity Hindering Cyber Tracking of Hackers*, PRESS ENTER. (June 18, 2011), http://www.pe.com/business/local/stories/PE_Biz_D_cyberlaw19.e4e25d.html (discussing FBI warnings of dangers).

173. *See* Glenn Derene *How Vulnerable is U.S. Infrastructure to a Major Cyber Attack?*, POPULAR MECHANICS (Oct. 30, 2009), http://www.popularmechanics.com/military/a4096/4307521/; Phil Stewart et al., *Special Report: Government in Cyber Fight, but Can't Keep Up*, REUTERS (June 17, 2011, 2:39 PM), http://www.reuters.com/article/us-usa-cybersecurity-idUSTRE75F4YG20110616.

hardening domestic networks rather than counter-attacks or other proactive measures.[174]

In a similar, if narrower, vein, the European Union's Parliament and Council adopted the Passenger Name Record (PNR) Directive in April 2016.[175] This Directive allows EU member states to enact legislation and regulations to establish how airlines will transfer passengers' data to national authorities. The data are to be collected and recorded for the purpose of investigating, detecting, and preventing "terrorist" incidents.[176] In order to achieve this goal, passengers' information must be transferred to immigration authorities before departure or arrival of a given flight to or from EU territory. Authorities may keep the passenger information for up to five years, but the data must be "depersonalized" six months after being collected.[177]

c. Data Retention

Many governments invest resources in monitoring online activities. The Indian government, for example, has decided to monitor services such as Twitter and Facebook for fear that "the services are being used by terrorists to plan attacks."[178] However, real-time monitoring is expensive. And even if social-networking sites, such as Twitter, present themselves as easy targets for monitoring because they aggregate a large quantity of communications from diverse sources, there are many other communications that are less public, but are frequently seen by governments as also potentially threatening.

Things happen quickly online and data can be erased. Thus, rather than having to anticipate the need to wiretap, or even react in real time, it would be much better for law enforcement if it were possible to turn back the virtual clock and wiretap the past in those cases where it seems necessary or convenient to do

---

174. *See* U.S. DEP'T OF DEFENSE, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE *passim* (2011), http://brendans-island.com/blogsource/20100402ff-Documents/d20110714cyber.pdf. The absence of an offensive strategy was noted by former Assistant Secretary of Homeland Security Stewart Baker who said, "The plan as described fails to engage on the hard issues, such as offense and attribution." Julian E. Barnes & Siobhan Gorman, *Cyberwar Plan Has New Focus on Deterrence*, WALL ST. J. (July 15, 2011), http://www.wsj.com/articles/SB10001424052702304521304576446191468181966.

175. *See* Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the Use of Passenger Name Record ("PNR") Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime, 2016 O.J. (L 119/132) [hereinafter EU PNR Directive]; European Council Press Release 176/16, Council Adopts EU Passenger Name Record (PNR) Directive (Apr. 21, 2016), http://www.consilium.europa.eu/press-releases-pdf/2016/4/40802210742_en.pdf.

176. *Regulating the Use of Passenger Name Record (PNR) Data*, EUR. COUNCIL, http://www.consilium.europa.eu/en/policies/fight-against-terrorism/passenger-name-record/ (last reviewed June 6, 2016).

177. *Id.*

178. John Ribeiro, *India Wants Special Monitoring Access for Twitter, Facebook*, PCWORLD (August 8, 2011, 20:33), http://www.pcworld.idg.com.au/article/396417/india_wants_special_monitoring_access_twitter_facebook/.

so. No time travel is needed, however, if governments can require communications intermediaries to keep copies of all their customers' communications. A large number of governments around the world have chosen to impose data retention by law, although there has also been resistance to these requirements.

Data-retention schemes rely on requiring intermediaries, usually private parties, to collect and store data on their customers. Leaving these pools of data in private hands means that if the government wants access to them it must, in theory, comply with the relevant legal rules. For example, in the United States, if the government wants access to stored communications it must obtain a court order, an action that in the ordinary case requires reasons and creates a paper trail. Although the subject of the court order may not be on notice in order to protect an ongoing investigation, in some cases the intermediary holding the data may have a chance to challenge the request if it seems overbroad.[179] The request may in some cases be subject to challenge before the court issues it;[180] in most cases the challenges can happen only if the government seeks to introduce the information it acquired in a later prosecution.[181] In a growing number of other cases, however, the U.S. government can use enhanced anti-terrorism powers, considerably reducing the power of the intermediary to challenge, or even mention, the existence, of the request.[182]

In the culmination of a campaign that started in 2006,[183] the FBI asked Congress to expand CALEA[184] to webmail, social-networking sites, and peer-to-peer services.[185] In each case, the goal would be to require companies involved in online communications to re-engineer their software so that law enforcement could easily access it.[186] In addition, the FBI has sought and received funding for its "Going Dark" project, which seeks legal and technical innovations to enhance lawful communications intercept capabilities.[187]

---

179. In the best-known example, trustees of a library district challenged a government administrative subpoena of library records via a national security letter and succeeded. *See Feds Drop Demand for Library Records*, NEWSTIMES (June 27, 2006, 1:00 AM), http://www.newstimes.com/news/article/Feds-drop-request-for-library-records-117718.php.

180. *See id.*

181. This is the so-called "exclusionary rule," which originated in *Weeks v. United States*, 232 U.S. 383 (1914) (providing the exclusionary rule for federal cases) and *Mapp v. Ohio*, 367 U.S. 643 (1961) (extending the exclusionary rule to the states).

182. *See, e.g.*, 50 U.S.C. § 1805(e)(1) (2012) (indicating that the Attorney General may authorize an emergency wiretap without prior approval by the FISA court).

183. *See supra* text accompanying notes 65–67.

184. Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001–1010 (2012).

185. *See FBI Seeks New Mandates on Communications Technologies*, CDT (Feb. 24, 2011) https://www.cdt.org/pr_statement/statement-concern-about-expansion-calea?quicktabs_4=1 (discussing CALEA and providing CDT's response).

186. Eric W. Dolan, *FBI Urges Congress to Expand Internet Wiretapping*, RAW STORY (Feb. 17, 2011, 21:39), http://www.rawstory.com/rs/2011/02/17/fbi-urges-congress-to-expand-internet-wiretapping/.

187. Current (2016) services for this initiative are 39 positions (11 agents) and $ 31 million. U.S. DEP'T OF JUSTICE, FY 2017 BUDGET REQUEST 2 (2016),

In 2011, the Obama Justice Department asked Congress to enact similar data-retention legislation in the United States,[188] although it left key details unspecified, leading to speculation that the Administration remained divided.[189] Subsequently, the Judiciary Committee of the U.S. House of Representatives passed a wide-ranging data-retention bill, labeling it the "Protecting Children From Internet Pornographers Act of 2011."[190] The proposal would require every "provider of an electronic communication service or remote computing service" to retain the temporarily assigned network addresses the service assigns to each account for at least 18 months, as well as account information about the customer.[191] As for the security aspects of this data, the proposed bill stated—nonbindingly—that, "[i]t is the sense of Congress that records retained pursuant to [§] 2703(h) of title 18, United States Code, should be stored securely to protect customer privacy and prevent against breaches of the records."[192] The bill also immunized covered service providers from liability for any disclosure of the information.[193] Alarmingly, the draft statute also permitted nonjudicial "administrative subpoenas" for the user data by the U.S. Marshals Service, albeit limiting that new power to investigations of "an unregistered sex offender."[194] The proposal did not become law.

Likewise, some Latin American countries have enacted legislation establishing systems for digital surveillance through the retention of data. The most prominent example of this is the Venezuelan Law on the Protection of Privacy of Communications enacted in 1991.[195] Article 6 of the statute empowers a

---

https://www.justice.gov/jmd/file/822286/download.

188. *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary* 112th Cong. (2011), https://www.justice.gov/sites/default/files/criminal-ceos/legacy/2012/03/19/Justice%20Data%20Retention%20Testimony.pdf (statement of Jason Weinstein, Deputy Assistant Att'y Gen.).

189. *See* John Morris, *DOJ Looking for Mandatory Internet Data Retention Law* CDT (Jan. 28, 2011), https://www.cdt.org/blogs/john-morris/doj-looking-mandatory-internet-data-retention-law.

190. *See* H.R. REP. NO. 112–281, pt. 1, at 3 (2011).

191. *See id.* at 4, § 4 (amending 18 U.S.C. § 2703 (2006)); Declan McCullagh, *House Panel Approves Broadened ISP Snooping Bill*, (July 28, 2011, 11:41 PM), http://news.cnet.com/8301-31921_3-20084939-281/house-panel-approves-broadened-isp-snooping-bill/ (discussing the legislation).

192. *Id.* § 4(b).

193. *Id.* § 5.

194. *Id.* § 11.

195. ACCESO LIBRE ET AL., STAKEHOLDER REPORT UNIVERSAL PERIODIC 26TH SESSION: THE RIGHT TO PRIVACY IN VENEZUELA 5 (2016), https://www.privacyinternational.org/sites/default/files/venezuela_upr2016.pdf; GACETA OFICIAL DE LA REPUBLICA DE VENEZUELA [OG] [OFFICIAL GAZETTE] No 34.863, LEY SOBRE PROTECCIÓN A LA PRIVACIDAD DE LAS COMUNICACIONES [Law on Protection of the Privacy of Communications] (Venez.) [hereinafter VENEZUELA PRIVACY LAW], http://venezuela.justia.com/federales/leyes/ley-sobre-proteccion-a-la-privacidad-de-las-comunicaciones/gdoc/ (translation on file with author). I am indebted to Jose Ponce for the translations from Spanish in this section.

broad range of security services, including intelligence agencies, to request a judicial order authorizing them to "prevent, interrupt, intercept or record communications" in order to investigate crimes against the "security and independence of the State," drug-related offenses, extortion and kidnapping, and crimes related to public finances.[196] However, the law does not obligate the Venezuelan security services or the courts to notify targeted persons that they are under surveillance, nor is there any rule limiting how long the state may store the data it collects.

The Venezuelan Government has extensive surveillance capabilities at its disposal. It has been employing FinFisher, a powerful spyware tool, since 2014.[197] And it is generally believed in Venezuela that the state-run National Telecommunications Commission monitors the online activities of social-network users.[198] Like Mexico,[199] Venezuelan law requires that all cellular-phone users register their SIM cards with a passport or identity card, fingerprint, signature, and address. [200] Venezuelan law also mandates that service providers create a SIM card database for each customer, and that they retain call records for up to three months after services have been discontinued.[201] Venezuelan security agencies can request the call registries.[202] Even the sale of basic goods, such as food and medicine,

---

196. VENEZUELA PRIVACY LAW, *supra* note 195, art. 6.

197. FinFisher is a spyware tool, sold exclusively to governments, which allows its users to effectively collect information on targeted subjects using disguised servers. *See* Bill Marczak et al., *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation*, CITIZEN LAB (Oct. 15, 2015), https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/.

198. ACCESSO LIBRE ET AL., *supra* note 195, at 12.

199. *See supra* text accompanying note 139.

200. ACCESSO LIBRE ET AL., *supra* note 195, at 13; OG No. 34.863, Normas Relativas al Requerimiento de Información en el Servicio de Telefonía Móvil [Rules Concerning the Requirement of Information in the Mobile Telephony Service], art. 5 (Venez.), http://www.conatel.gob.ve/providencia-%20administrativa-572-normas-relativas-al-requerimiento-de-informacion-en-el-servicio-de-telefonia-movil-ano-2005/ (translation on file with author).

201. *Id.* art. 4 ("Data Retention: For the purposes of State Security Services requiring service providers to provide them with data, in the context of criminal investigations, the documents provided by service subscribers, referred to in Article 2 of this Regulation, must available in physical form, at least for 2 years from the date they were obtained by the service provider. After this period of time, the documents can be discarded provided that the documents have been digitalized or stored in microfilm, ensuring that they are legible, especially the finger print impression."). In addition, service providers are required to keep this information archived while the corresponding subscriber's contract is in force and three months after it has been concluded. *See id.*

202. *Id.* art. 7 ("For the purposes of providing State Security Services with information they request during criminal investigations, service providers are to have at their disposal, at the moment when such information is requested, the registry of phone calls made by their subscribers in the previous three months. This information is to be provided immediately after being requested . . . . In any case, service providers shall store the registry of calls made by their subscribers during the last 12 months, before the three month period established herein. This information has to be provided to State Security Services thirty calendar days after being requested . . . .").

require that buyers submit their biometric data at the point of sale.[203] The use of similar biometrics for elections has led to public skepticism about the integrity of both the biometric data collection systems and monitoring in connection with the electoral process.[204]

European law in many states now requires telephone companies, ISPs, and other intermediaries to archive information about the communications—email headers and call setup data—of their customers for periods of six months to two years.[205] Most of these rules result from national implementation of the Directive on Mandatory Retention of Communications Traffic Data ("EU Data Retention Directive" or "EU Directive"),[206] although implementation has been uneven and controversial at the member-state level, and was further complicated by the European Court of Justice's 2014 ruling striking down the Directive.[207]

The European Union originally adopted the EU Data Retention Directive in March 2006,[208] despite opposition in the European Parliament.[209] To prevent, investigate, detect, and prosecute serious crimes, such as organized crime and terrorism,[210] the now-invalidated EU Directive required the providers of publicly available electronic communications services or public-communications networks to retain traffic and location data belonging to individuals or legal entities. These data included the calling telephone number, name, and address of the subscriber or registered user; user IDs (a unique identifier assigned to each person who signs with an electronic-communications service); Internet Protocol addresses; the numbers dialed; and call forwarding or call transfer records.[211] The Directive instructed member states to require communications providers to retain these communications data for a period of between six months and two years, starting no later than March 2007.

The Directive survived an initial challenge in the ECJ.[212] However, the Directive met with resistance in several European states, and there were disputes and domestic court challenges to its implementation.[213] Several member states failed to implement the directive by the 2007 deadline, leading to declarations by

---

203. ACCESO LIBRE ET AL., *supra* note 195, at 13–15.

204. *Id.*

205. *See* Directive 2006/24/EC, of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105), arts. 3–6 [hereinafter EU Data Retention Directive].

206. *Id.*

207. *See* Joined Cases C-293/12 & C-594/12, Digital Rights Ir. Ltd. v. Minister for Commc'ns, Marine & Nat. Res., 2014 E.C.R. I-238.

208. *See* EU Data Retention Directive, *supra* note 205.

209. *See* Christian DeSimone, *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*, 11 GER. L.J. 291, 301 (2010).

210. EU Data Retention Directive, *supra* note 205, art. 1 §1, art. 6.

211. *Id.* art. 5.

212. Case C-301/06, Ireland v. European Parliament, 2009 E.C.R I-593.

213. *See* Brown, *supra* note 128, at 96.

the ECJ against Austria,[214] Greece,[215] Ireland,[216] and Sweden.[217] A leading example of national legal resistance came in the 2010 decision of the German Federal Constitutional Court ("BVerfG") which nullified key parts of the German law implementing the Directive.[218] The court faulted the law for its lack of data security, transparency, and legal protections, holding that it was therefore disproportionate and unconstitutional. The court left in place those parts of the law that it thought were required by the Directive, but struck down the parts that it found to exceed the EU mandate.[219] The decision caused the Commission to announce it would reconsider the Directive,[220] and it set up a consultative process.[221]

European governments defended their data-retention laws against creative challenges. In anticipation of Sweden's implementation of the EU Data Retention Directive, in 2011 Swedish ISP Bahnhof designed its systems so that even it could not tell what its customers were doing. As a result, the company had no data that could be subject to a data-retention regime. To gild the lily, Bahnhof charged its customers an $8.00 per-month premium to have a traditional, surveillance-friendly internet connection, instead of an anonymous proxy.[222] Sweden then imposed a data-retention regime, only to have it first struck down and then reinstated by its national courts. Thus in 2014, some months after the ECJ's decision striking down the Directive, the Swedish statute was again in force and Bahnhof faced a fine of 5 million Swedish krona (about $676,000) under Swedish law if it refused to resume collecting customer metadata.[223] Bahnhof responded by filing a complaint with the EU Commission,[224] and offering users free anonymous VPN accounts in order to

---

214. Case C-189/09, European Comm'n. v. Austria, 2010 E.C.R. I-99.

215. Case C-211/09, European Comm'n. v. Hellenic Rep., 2009 E.C.R. I-204.

216. Case C-202/09, European Comm'n v. Ireland, 2009 E.C.R. I-203.

217. Case C-185/09, European Comm'n v. Sweden, 2010 E.C.R. I-14, 32–33.

218. *See* DeSimone, *supra* note 209, at 314–15.

219. *Id.* at 315–16; *see also* Press Release, Bundesverfassungsgericht [Fed. Constitutional Court], Data Retention Unconstitutional in its Present Form (Mar. 2, 2010), https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html.

220. DeSimone, *supra* note 209, at 317; *see also* European Comm'n, Justice, Review of the data protection legal framework, [http://web.archive.org/web/20101107205134/http://ec.europa.eu/justice/policies/privacy/review/index_en.htm] (promising "[l]egislation will be put forward in 2011").

221. *See, e.g.*, *European Parliament Meeting Offers Update on Review of EU Data Protection Directive*, PRIVACY & SECURITY L. BLOG (Mar. 16, 2011), http://www.huntonprivacyblog.com/2011/03/articles/european-union-1/european-parliament-meeting-offers-update-on-review-of-eu-data-protection-directive/.

222. *See* Enigmax, *Wikileaks ISP Anonymizes All Customer Traffic to Beat Spying*, TORRENT FREAK (Jan. 27, 2011), https://torrentfreak.com/wikileaks-isp-anonymizes-all-customer-traffic-to-beat-spying-110127/.

223. Liam Tung, *Swedish Data Retention Back in Full Swing Minus One ISP*, ZDNET (Oct 29, 2014, 16:59), http://www.zdnet.com/article/swedish-data-retention-back-in-full-swing-minus-one-isp/.

224. Loek Essers, *Swedish ISP Urges European Commission to End 'Illegal Data Retention'*, COMPUTERWORLD UK (Sept 12, 2014),

circumvent the Swedish law as the metadata it collected would be of little or no value.[225]

Then, in April 2014, in a "landmark ruling"[226] involving a reference from Irish and Austrian courts, the ECJ declared the Directive invalid.[227] The ECJ held that the Directive exceeded the limits of proportionality by entailing serious interference with rights to privacy and personal-data protection guaranteed by the Charter of Fundamental Rights. The ECJ also faulted the Directive for failing to require prior review by a judicial or other independent administrative authority before giving governments access to the retained customer data.[228]

"Because the ECJ did not specify otherwise, the Data Retention Directive is void ab initio and EU Members who have transposed the Directive into their national legal systems must ensure compliance with the ECJ's judgment."[229] In other words, national legislation based on or anticipating the Directive does not become void when the Directive is voided; rather the national legislation becomes subject to challenge under the relevant national law and perhaps EU law also. Thus, defenders of purportedly implementing national legislation could no longer defend those statutes based on the existence of the Directive, which would have had precedence over contrary national rules due to the EU treaties. Furthermore, the ECJ's decision invalidating the Directive suggested that instead of supporting the laws designed to implement the Directive, EU law would henceforth serve as grounds for invalidating some aspects of those laws, although the issue is murkier than a cognate constitutional case would be in the United States.

In March 2015, the EU Commission signaled that it did not intend to introduce a revised version of the Directive.[230] Instead, in 2016 the EU committed itself to a new General Data Protection Regulation (GDPR) that will take effect in 2018.[231] The GDPR's primary focus is on data not speech; thus, the GDPR does not protect a right to anonymous speech, although it does encourage the

---

http://www.computerworlduk.com/news/it-business/3571873/swedish-isp-urges-european-commission-to-end-illegal-data-retention/.

225. Douglas Crawford, *Renegade Swedish ISP Offers All Customers VPN*, BESTVPN (Nov. 18, 2014), https://www.bestvpn.com/blog/11806/renegade-swedish-isp-offers-customers-vpn/.

226. Marie-Pierre Granger & Kristina Irion, *The Court of Justice and the Data Retention Directive in* Digital Rights Ireland*: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, 39 EUROPEAN L. REV. 835, 849 (2014).

227. Joined Cases C-293/12 & C-594/12, Digital Rights Ir. Ltd. v. Minister for Commc'ns, Marine & Nat. Res., 2014 E.C.R. I-238.

228. *Id.*

229. LAW LIBRARY OF CONG., EUROPEAN UNION: ECJ INVALIDATES DATA RETENTION DIRECTIVE 1 (2014), http://www.loc.gov/law/help/eu-data-retention-directive/eu.php.

230. Francesco Guarascio, *EU Executive Plans No New Data Retention Law*, REUTERS (Mar 12, 2015, 2:28 PM), http://www.reuters.com/article/2015/03/12/us-eu-data-telecommunications-idUSKBN0M82CO20150312.

231. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119).

psedonymization of 'personal data' more generally.[232] Indeed, the GDPR disclaims applicability to truly anonymous activities, since (barring re-identification) there is no personal data at stake.[233] In contrast, the GDPR will likely have a significant impact on EU member state data retention rules as it requires more explicit consent for data collection, and requires that the consent be easily revocable.[234]

Pending the transition to the GDPR in 2018, the status of various EU member states' laws enacted on the basis of the Privacy Directive remains in flux, as the fight moves to—or returns to—the various member states' courts. One early indication that older rules may fare poorly in the new environment was a judgment of the Dutch court of first instance, which struck down the Netherlands's more sweeping data retention rule, one that the court said could in theory be applied to the prevention of bike thefts; whether the government will seek to pass a narrower law is unclear.[235]

Germany enacted a data-retention law requiring telecommunication and internet providers to store customer metadata and provide the metadata to law enforcement agencies investigating "severe crimes."[236] Providers will be required to retain phone numbers, the date and time of phone calls and texts, text messages, the locations of cell phone call participants, IP addresses, port numbers and the date and time of Internet access.[237]

In what Edward Snowden called "the most extreme surveillance in the history of western democracy… [that] goes farther than many autocracies," [238] the UK surpassed Germany by enacting an even more sweeping data-retention requirement in November 2016. After years of debate, the UK Parliament adopted the Investigatory Powers Act 2016,[239] a wide-ranging revision of its surveillance law. Dubbed the "snooper's charter" by its critics, the Act requires ISPs to record every internet customer's top-level web history in real-time and keep the records

---

232. *Id.* paras. 26, 28, 29; *id.* arts. 25(1), 32(1)(a).

233. *Id.* para. 26 ("The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.").

234. *Id.* paras. 32, 43; *id.* art. 1(a) (consent required); *id.* art. 6(4) (legal requirements to process data without consent must be proportionate to the public democratic purpose); *id.* art. 7 (defining terms for consent and withdrawal of consent); *id.* art. 9 (public interest exceptions).

235. Guest Author, *Dutch Data Retention Law Struck Down – for Now*, EDRI (Mar. 12, 2015), https://edri.org/dutch-data-retention-law-struck-down-for-now/.

236. Glyn Moody, *Proposed German Law: Telecoms Must Store Customer Data on Airgapped Servers*, ARS TECHNICA (Oct. 21, 2015, 12:10 PM), http://arstechnica.com/tech-policy/2015/10/german-parliament-passes-new-comprehensive-data-retention-law/; Eric J. Shinabarger, *New German Data Retention Law Expected to Take Effect Soon*, LEXOLOGY (Jan. 13, 2016), http://www.lexology.com/library/detail.aspx?g=fe41234a-b807-47da-a20e-b725327b537a.

237. *Id.*

238. Edward Snowden (@Snowden), TWITTER (Nov. 17, 2016, 2:59 PM), https://twitter.com/Snowden/status/799371508808302596.

239. Investigatory Powers Act 2016, c. 25 (UK), http://www.legislation.gov.uk/ukpga/2016/25/introduction/enacted.

for up to a year while making them available to several government departments.[240] The Act will also require companies to decrypt their customers' data on demand if they are able to do so.[241] The government justified the mandatory decryption requirement on the grounds that it would give investigators the same level of access to people's online communications that the government currently has to more traditional means of communication.[242] However, if the GDPR comes into effect in the UK before the UK leaves the EU , which seems likely given that the GDPR's effective date in 2018 precedes the earliest projected date of any "Brexit," the GDPR will conflict with the Investigatory Powers Act so long as the UK is under EU law—and perhaps beyond then—the GDPR would control.[243] Data-retention laws in other EU member states such as Germany could also face similar conflicts with the GDPR's requirements that persons specifically consent to data collection and processing, and that they have the right to withdraw that consent as easily as they gave it.[244]

Data-retention efforts are by no means limited to the EU. In 2012, Australia passed Cybercrime Legislation Amendment Bill 2011, which it described as needed to allow Australia to enter into the Council of Europe Convention on Cybercrime.[245] Critics of the bill claimed that it goes well beyond the information-sharing aspects of the Convention and could lead to the ongoing collection and retention of private communications. Unlike the Convention, which contains an exception to its general data-sharing policy if a government finds that the data being requested by a foreign power relates to a political offence or if sharing it would contravene human rights standards, the Australian act has no such

---

240. Allen Travis, *Investigatory Powers Bill: The Key Points*, GUARDIAN (Nov. 4, 2015, 8:04 PM), https://www.theguardian.com/world/2015/nov/04/investigatory-powers-bill-the-key-points.

241. The original bill required providers of services with end-to-end encryption to install back doors into their products and services. The final draft only required them to decrypt if they had the capability to do so. *See Investigatory Powers in 'Ping Pong'*, CLAYDEN LAW (Nov. 11, 2016), http://www.claydenlaw.co.uk/site/library/clayden-law-news/investigatory-powers-bill-in-ping-pong.

242. Nicholas Watt, *David Cameron: 'Snooper's Charter' will Re- Appear after After Tory Election Win*, GUARDIAN (Jan. 11, 2015, 15:39), http://www.theguardian.com/politics/2015/jan/11/david-cameron-snoopers-charter-tory-election-win; Nicholas Watt et al., *David Cameron Pledges Anti-Terror Law for Internet After Paris Attacks*, GUARDIAN (Jan. 12, 2015, 17:04), http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg; Matt Burgess, *Cameron Might Fast-Track Snooping Bill After Paris Attacks*, WIRED (Nov. 16, 2015), http://www.wired.co.uk/news/archive/2015-11/16/cameron-fast-track-surveillance-investigatory-powers-bill.

243. *See* Pascal Crowe, *Could the European GDPR Undermine the UK Investigatory Powers Act?*, MEDIA POL'Y PROJECT: BLOG (Dec. 19, 2016), http://blogs.lse.ac.uk/mediapolicyproject/2016/12/19/could-the-european-gdpr-undermine-the-uk-investigatory-powers-act/.

244. *See supra* note 234.

245. *Cybercrime Legislation Amendment Bill 2011*, PARLIAMENT OF AUSTL., http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4575 (last visited Jan. 16, 2017).

exemptions.[246] Just before the passage of the Act in August 2012, Australian Attorney-General Nicola Roxon announced a two-year delay on any plans to require ISPs to store the web history of all their customers.[247]

Then, in March 2015, the Australian Parliament passed the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015,[248] which requires all Australian telecommunications providers to keep all metadata associated with customer communications for two years. The Bill also establishes procedures for the secure storage of that data, and for government access to it, with an effective date in 2017.

Developments in the Russian Federation are perhaps the most negative. In June 2016, President Vladimir Putin signed the so-called Yarovaya Law, creating new surveillance powers for Russian security services. The law amends existing counter and anti-terrorist legislation in order to require cellular-phone carriers, ISPs, and messaging-application-service providers to store all communications data for six months; metadata has to be stored for three years. Worse, cryptographic backdoors are now mandatory in all messaging applications.[249] The amendments also established criminal liability for people who do not report someone who is purportedly involved in the planning or execution of "terrorist" acts.[250] Somehow, the Federal Assembly of the Russian Federation adopted these rules[251] despite the strict prohibitions in Russia's Constitution against the retention of individuals' personal information, under any circumstances.[252]

---

246. *See* Explanatory Memorandum, Inquiry into Cybercrime Legislation Amendment Bill 2011 (Cth) (Austl.), http://www.austlii.edu.au/au/legis/cth/bill_em/clab2011314/memo_0.html.

247. Philip Dorling, *Roxon Puts Web Surveillance Plans on Ice*, AGE (Aug. 10, 2012), http://www.theage.com.au/technology/technology-news/roxon-puts-web-surveillance-plans-on-ice-20120809-23x9l.html.

248. *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015*, PARLIAMENT OF AUSTL., http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5375 (last visited Jan. 16, 2017).

249. Ilya Khrennikov, *Putin's 'Big Brother' Surveillance Law Criticized by Snowden*, BLOOMBERG TECH. (Jul. 7, 2016, 5:35 AM), http://www.bloomberg.com/news/articles/2016-07-07/putin-s-anti-terror-law-sends-telecommunications-companies-lower.

250. Tany Lokoshina, *Draconian Law Rammed Through Russian Parliament*, HUMAN RIGHTS WATCH (Jun. 23, 2016, 12:34 PM), https://www.hrw.org/news/2016/06/23/draconian-law-rammed-through-russian-parliament.

251. *See* Evgeniya Melnikova, *Yarovaya Law: The Death of the Russian Constitution*, WORLD POST (Jul. 11, 2016, 5:49 PM), http://www.huffingtonpost.com/evgeniya-melnikova/yarovaya-law-the-death-of_b_10864882.html.

252. *See* KONSTITUTSIIA ROSSIISKOI FEDERATSII [KONST. RF] [CONSTITUTION] arts. 23–24, 28 (Russ.). The Russian Constitution provides as follows:

> Article 23
>
> 1. Everyone shall have the right to the inviolability of private life, personal and family secrets, the protection of honour and good name.

Not to be outdone, in early 2017 China banned "unauthorized" VPNs, "i.e. ones without backdoors that the authorities can use to tap communications."[253] in order to preserve surveillance capacity and to stamp out attempts to route around Chinese censorship.

As this incomplete survey demonstrates,[254] there is a simultaneous and, in some sense, concerted push on multiple continents to create a legal regime in which communications will logged, if not actually recorded, and their metadata stored. The mechanisms for this logging and storing are in addition to—and redundant to—the efforts of the NSA and its partners, but are designed to make that information available to a much wider variety of agencies in a much larger number of countries. Perhaps at first the data retained will be available only to law enforcement and other national authorities for "the prevention, detection, investigation, and prosecution of terrorist offenses and serious crime."[255] Function creep, however, is all but inevitable.

III. PREPARING FOR THE NEXT WAVE: TIME TO RE-LEARN OLD LESSONS

As Part II demonstrated, the abolition of online anonymity is now a real possibility, both technically and legally. This Part explains why that would be unfortunate and sketches what we can do about it.

> 2. Everyone shall have the right to privacy of correspondence, of telephone conversations, postal, telegraph and other messages. Limitations of this right shall be allowed only by court decision.
>
> Article 24
>
> 1. The collection, keeping, use and dissemination of information about the private life of a person shall not be allowed without his or her consent.
>
> 2. The bodies of state authority and local self-government, their officials shall ensure for everyone the possibility of acquainting with the documents and materials directly affecting his or her rights and freedoms, unless otherwise provided for by law."
>
> Article 28
>
> Everyone shall be guaranteed the freedom of conscience, the freedom of religion, including the right to profess individually or together with other any religion or to profess no religion at all, to freely choose, possess and disseminate religious and other views and act according to them.

Id.

253. Graeme Burton, *China Makes VPNs that Bypass Great Firewall Illegal*, INQUIRER, (Jan. 24, 2017), http://www.theinquirer.net/inquirer/news/3003139/china-makes-vpns-that-bypass-great-firewall-illegal.

254. For an international survey of journalists' and bloggers' rights to write anonymously, see Jason A. Martin & Anthony L. Fargo, *Anonymity as a Legal Right: Where and Why It Matters*, 16 N.C.J.L. & TECH. 311 (2015).

255. *See* EU PNR Directive, *supra* note 175, at 132.

A. Why Anonymity Matters

Communicative anonymity is a core part of freedom in a democratic state and a critical tool for those who seek freedom from nondemocratic states. The rapid deployment of profiling and surveillance technologies in both the public and private sectors only increases the importance of preserving the ability to be anonymous: without it, every utterance, every purchase, and every computer-mediated interaction risks becoming part of one's dossier. There are profound differences between dossiers kept by marketers, by benign governments, and by malign ones, but in every case without the ability to be anonymous at least sometimes, life becomes a continuous experience of being watched and recorded. The existence of profiling databases, whether in corporate or public hands, constricts the economic and, in some places, the political freedoms of the persons profiled; profiling not only increments the amount of data in existence about a person, but by organizing the data into easily searchable form it also reduces her effective privacy via data mining. Anonymity is the escape hatch. Allow—or worse, legislate or demand—a communications architecture without this option, and we will have set our course towards the goldfish-bowl society.[256]

First-wave internet regulation could never have achieved the identification of every user and every data packet. The second wave is and was both more international and more adept; when law harnesses technology to its ends law can achieve far more than when it either regulates outside technology (categorization) or regulates against it. As these techniques are further perfected and deployed, it becomes increasingly practical to not only counteract the aspects of computer-mediated communication that made anonymity easy, but in fact to make anonymous communication more difficult than ever. A 2011 European Center for Political Economy report notes the spreading governmental drive to control communications:

> The forebodings about censorship spreading to other areas of technology have proven to be justified. An entire new range of services, for example software sales through mobile networks (so-called apps), e-books, and licenses for cheap Internet calls via VOIP (such as Skype, MSN messenger and Google Talk) are restricted and eavesdropped.[257]

The consequences risk being severe. More than a decade ago, the Internet seemed poised to serve libertarian values; a decade ago some of us thought they might, with some pushing, be Habermasian.[258] The future looks more grim, threatening to vindicate earlier Foucaultian predictions. The challenge for theorists and activists is to structure the coming era of inescapable tracking and information so that we at least have a responsible society, one in which the democracy-enhancing aspects of internet technology are nurtured, and not one where, as is too common in times of fear and hardship, authorities become empowered at the expense of all citizens.

---

256. *See* Froomkin, *supra* note 60, at 507; Froomkin, *supra* note 1, at 1465.
257. Erixon & Lee-Makiyama, *supra* note 72, at 15.
258. *See* Froomkin, *supra* note 26.

In many countries, the power to prevent anonymity, to force identification, and to gather traffic data for analysis will be used to stamp out dissidents. We should admit that sometimes those dissidents may be terrorists; technology can empower very bad people as well as very good ones. But that is also this Article's point: sometimes the very bad people are in power, and the people against whom they will use technologies of identification are the human rights activists, the democratic and nonviolent protestors, and the Twitter users planning demonstrations.[259] And after the technologies of identification will come the technologies of retaliation.

The U.S. government does not seem to be of one mind on these questions. During her term as Secretary of State, Hillary Clinton spoke more than once about "21st Century Statecraft"[260] and the importance of communicative freedom in spreading democracy and development. She was careful to note that anonymity allows the theft of intellectual property, but also pointed out that anonymity "permits people to come together in settings that give[] them some basis for free expression without identifying themselves" and concluded that "[w]e should err on the side of openness." [261]

Similarly, President Barack Obama stated in 2015 that he is "a strong believer in strong encryption." He went on to say, "I lean probably further on the side of strong encryption than some in law enforcement," and "[t]here's no scenario in which we don't want really strong encryption." Unfortunately, only a year later, President Obama backpedaled from this position. Speaking alongside British Prime Minister Cameron, he argued that, "[i]f we find evidence of a terrorist plot . . . and despite having a phone number, despite having a social media address or email address, we can't penetrate that, that's a problem."[262] Even more recently, President Obama's Justice Department took an aggressive stand against Apple, seeking to use the All Writs Act in a manner that would not only require

---

259. One should not, however, go overboard. There is evidence, for example, that shutting down the Internet actually assisted revolutionaries in Egypt as it forced them to organize in decentralized local groups that were harder to track, and which developed strong personal loyalties able to withstand government opposition. *See* Navid Hassanpour, *Media Disruption Exacerbates Revolutionary Unrest: Evidence from Mubarak's Quasi-Experiment*, 31 POL. COMM. 1 *passim* (2014), http://dx.doi.org/10.1080/10584609.2012.737439.

260. Hilary Rodham Clinton, U.S. Sec'y State, Remarks on Internet Freedom at The Newseum (Jan. 21, 2010), (Transcript available at http://web.archive.org/web/20100123145341/http://www.state.gov/secretary/rm/2010/01/135519.htm).

261. *Id.*; *see also* SAM DUPONT, CONNECTION TECHNOLOGIES IN U.S. FOREIGN POLICY: AN OVERVIEW OF 21ST CENTURY STATECRAFT & INTERNET FREEDOM (2010), http://ndn.org/sites/default/files/paper/TechnologyInForeignPolicy.pdf (summarizing State Department's "21st Century Statecraft" and "Internet Freedom" initiatives); *21st Century Statecraft*, U.S. DEP'T STATE (Jan. 7, 2017), [http://web.archive.org/web/20170107231129/https://www.state.gov/statecraft/overview/index.htm].

262. Danny Yadron, *Obama Sides with Cameron in Encryption Fight*, WALL ST. J. (Jan. 16, 2015, 4:52 PM), http://blogs.wsj.com/digits/2015/01/16/obama-sides-with-cameron-in-encryption-fight/.

Apple to defeat a cell phone's security system, but that also threatened to set a precedent suitable for requiring firms to help the government undermine encryption systems they sold to their customers.[263]

In 1983, Ithiel de Sola Pool wrote presciently about networking technology:

> Technology will not be to blame if Americans fail to encompass this system within the political tradition of free speech. On the contrary, electronic technology is conducive to freedom. . . . Computerized information networks of the twenty-first century need not be any less free for all to use without hindrance than was the printing press. Only political errors might make them so.[264]

History teaches us that these errors are most likely made in periods of hysteria. And we in the United States have just lived through—or may still be living through—one such period of hysteria following the 9/11 tragedy, which itself took place about 15 years ago. How much has returned to normal since "9/11 changed everything" is open to question. Consider the furor over WikiLeaks, and then consider that even if the costs of making those records public outweighed the benefits, it is already clear that at least the U.S. government's and U.S. media's panicked responses were undoubtedly excessive. Consider also the more recent major controversy and legal battle regarding Apple's refusal to unlock an iPhone belonging to one of the known perpetrators of the San Bernardino mass shooting in December 2015.[265] And, most consequentially, consider the election of November 2016. The Trump administration's early actions show a commitment to stoking fear to justify its policies,[266] one of the indicators of a totalitarian, even fascist, governance style.[267] If that tendency were to manifest itself more strongly in the

---

263. *See A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/; Jacob Gershman, *Apple v. Justice Department: Politicians and Activists Take Sides on Encryption Order*, WALL ST. J. (Feb. 17, 2016, 2:51 PM), http://blogs.wsj.com/law/2016/02/17/apple-v-justice-department-politicians-and-activists-take-sides-on-encryption-order/; Danny Yadron et al., *Inside the FBI's Encryption Battle with Apple*, GUARDIAN (Feb. 18, 2016, 1:00 PM), http://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple; *see also* Order Compelling Apple, Inc. to Assist Agents in Search, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M (C.D. Cal. Feb. 16, 2016) (ordering Apple to cooperate with government agents' efforts to unlock an iPhone seized at the scene of the San Bernardino shooting).

264. ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM: ON FREE SPEECH IN AN ELECTRONIC AGE 231 (1983).

265. *See* sources cited *supra* note 263.

266. *See* Karen Tumulty & David Nakamura, *Trump's Rallying Cry: Fear Itself*, WASH. POST (Feb. 3, 2017), https://www.washingtonpost.com/politics/trumps-rallying-cry-fear-itself/2017/02/03/7d2a0432-ea4a-11e6-bf6f-301b6b443624_story.html.

267. *See* Isaac Chotiner, *Is Donald Trump a Fascist?*, SLATE (Feb. 10, 2016), http://www.slate.com/articles/news_and_politics/interrogation/2016/02/is_donald_trump_a_fascist_an_expert_on_fascism_weighs_in.html (interviewing Robert Paxton, Columbia University, Mellon Professor Emeritus of Social Science); John W. Whitehead, *Does Fear Lead to Fascism? A Culture of Fear and the Epigenetics of Terror*, RUTHERFORD INST. (Dec. 7, 2015),

future, then the channel for dissent preserved by anonymity and communications privacy generally will become more imperiled—and more important.[268]

Even before the election, anonymity and communicative privacy had a diverse coalition ranged against them. As we have seen, in the United States, fans of mandatory identification include the military, who worry about cyber terrorism; the police, who want easier ways to catch bad guys; publishers who want to protect established business models; people subjected to anonymous libel who understandably want to find their victimizers; and marketers salivating at the thought of systems designed to make every internet move recordable, accessible, and subject to data mining. Now to that list we can add the new Attorney General who, while a Senator, strongly opposed private access to encryption capable of preventing government access to communications.[269]

The most vocal critics of anonymous communication include some law professors—notably, feminists and progressives—who argue that anonymity is not just a cloak behind which the social oppressor hides. These critics argue that anonymity empowers and intoxicates pathological personalities and thus makes them more likely to engage in hate speech or to silence women or minorities.[270] It follows that we should eliminate anonymity by requiring intermediaries, the ISPs, to keep logs of their visitors so that we can track the perpetrators. And, in some cases, it is suggested that those hosting open forums should act as cyber-censors or face consequences for distributor liability, in effect enlisting private parties as unpaid regulators.[271]

It is striking how many different governments around the world have, in the past decade, brought forward proposals or initiatives designed to reign in the communicative freedom of their citizens or to strengthen the ability of state police and intelligence services to access what people say and do online (and by telephone), both in real time and well after the fact. The urge to take names is found among both democrats and despots. These governmental efforts arise from a combination of forces, with the desire to stamp out dissent—not to mention

---

https://www.rutherford.org/publications_resources/john_whiteheads_commentary/does_fear_lead_to_fascism_a_culture_of_fear_and_the_epigenetics_of_terror.

268. *See Trump Election Ignites Fears Over U.S. Encryption, Surveillance Policy*, FORTUNE (Nov. 10, 2016), http://fortune.com/2016/11/09/trump-encryption-surveillance-policy/ (reporting fears of "technology companies and civil libertarians . . . that a self-described 'law and order' president will attempt to expand surveillance programs and rejoin a long-running battle over government access to encrypted information.").

269. Russel Brandom, *Trump's Attorney General Pick Could Restart the Encryption Fight*, VERGE (Nov. 18, 2016), http://www.theverge.com/2016/11/18/13677798/attorney-general-jeff-sessions-encryption-san-bernardino-trump.

270. *See* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 83 (2009); Martha C. Nussbaum, *Objectification and Internet Misogyny*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 68, 85 (Saul Levmore & Martha C. Nussbaum eds., 2010). *But see* J. Nathan Matias, *The Real Name Fallacy*, CORAL PROJECT (Jan. 3, 2017), https://blog.coralproject.net/the-real-name-fallacy/ (arguing that group norms rather than real name policies determine online behavior).

271. *See* Citron, *supra* note 270, at 122–25.

sedition, a common but not inevitable factor. More legitimate motivations include international worries about terrorism and crime, and state-level worries about the same. These concerns sometimes dovetail with corporate worries about a number of online activities ranging from hacking to unlicensed digital copying ("piracy") and anonymous attacks on corporate activities, including some that move markets. To these one might add the concerns raised by radical attempts to create transparency through public posting of national and corporate secrets, of which WikiLeaks is perhaps the most notorious.

In the face of all these disparate voices and interests, so many of which are legitimate and so many of which are powerful (and a few of which are even both legitimate and powerful), is there still a viable case for protecting online anonymous speech and trying to prevent real-time tracking of our movements in both cyberspace and three-dimensional life? Yes. The case for preserving the option of communicative anonymity is both legal and practical, and very international.

B. Legal Counterweights

As we have seen, the case for regulating anonymity, and thus for identification and data retention, is based on familiar elements, including a strong dose of familiar means-ends arguments claiming increased security or efficiency. Many of the counterarguments draw from familiar sources also: claims that municipal and international law limit governments' rights to impose these restrictions on private communications are based on familiar texts and time-tested foundational legal principles. Here, however, familiarity should breed respect. As always, the risk is that doctrine has a tendency to bend in the face of perceived emergencies—or it may be ignored altogether.

With regard to U.S. law, the constitutional case is straightforward. It is settled constitutional law that the rights to anonymous speech and association are key protections for members of threatened minorities and unpopular organizations.[272] And there is also a line of cases starting with *Talley v. California*,[273] then *McIntyre v. Ohio Elections Commission*,[274] and running through the later *Watchtower Bible and Tract Society*,[275] in which the Supreme Court made it clear that there is a sweeping constitutional right to anonymous religious and political speech. Any wholesale bans on anonymous speech, including the very restrictions cheered by some progressive activists, would reach this zone of core First Amendment speech and are therefore unconstitutional—at least until the doctrine bends. Technology introduces complexity: for better or worse, once it is encrypted there is no way to distinguish religious or political speech from other speech online—there is no reliable "politics bit." So if one

---

272. NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 454 (1958). Some state constitutional rights to privacy may also protect anonymous speech. *See, e.g.*, Thaddeus Houston, *Constitutional Drag Race: Anonymous Online Speech After* Digital Music News v. Superior Court, 30 BERKELEY TECH. L.J. 1243, 1261–65 (2015).

273. 362 U.S. 60 (1960).

274. 514 U.S. 334 (1995).

275. 536 U.S. 150 (2002).

wants to protect anonymous political speech, it turns out that the only way to do this effectively is to be ready to protect all speech.[276] And that is perhaps the bitter pill the Obama Administration appeared to understand, but struggled with swallowing.[277]

We are already well past the day when the United States dominated the Internet, and it is highly likely that the United States will only become less central as an internet intermediary and traffic hub in the next decade. It does not immediately follow, however, that U.S. law will become that much less relevant to internet freedom. Users in other countries are able to continue to host content in the United States and to access otherwise forbidden content via proxies and other intermediaries in the United States (or any other equally well-connected nations with liberal rules on content) so long as they are able to get past domestic rules and technologies that seek to identify them. But it is precisely this point of vulnerability that new regulatory strategies and new technologies seek to take advantage of—and that new technological countermeasures seek to defeat.

As a result, international legal rules relating to free expression could take on additional importance. EU law has a chance to be a leader here, depending in part on whether the ECJ's decision invalidating the Data Retention Directive becomes the model for corralling the many European national laws requiring data retention.[278] Several other transnational agreements with broader membership also refer to the right to speak freely, a right that extends naturally to the rights to speak anonymously and the right not to have one's communications archived against one's will.

The clearest example is Article 19 of the Universal Declaration of Human Rights, which provides, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[279] The Universal Declaration can perhaps be disparaged as only "soft law," but in the Helsinki Final Act the 56 participating states agreed to "act in conformity with the purposes and principles of the . . . Universal Declaration of Human Rights."[280] They also recognized "the importance of the dissemination of information from the other participating States" and agreed to "make it their aim to facilitate the freer and wider dissemination of information of all kinds" as well as "encourage co-operation in the field of information and the exchange of information with other countries."[281]

---

276. *See* A. Michael Froomkin, *From Anonymity to Identification*, 1 J. SELF-REG. & REG. 120, 130 (2015), https://journals.ub.uni-heidelberg.de/index.php/josar/article/view/23480.

277. *See supra* Section II.B.2.b.

278. *See supra* Section II.C.

279. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 19 (Dec. 10, 1948).

280. Conference on Security and Cooperation in Europe: Final Act, Aug. 1, 1975, 14 I.L.M. 1292, 1295, http://www.osce.org/helsinki-final-act?download=true.

281. *Id.* at 1315.

Similar rights to communicative freedom appear in a more summary, or more qualified form, in other international agreements,[282] such as in Article 19 of the International Covenant on Civil and Political Rights, which states:

> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (*ordre publique*), or of public health or morals. [283]

The strong provisions of Article 8, section 1 of the European Convention on Human Rights might seem to ban all data retention, providing that: "Everyone has the right to respect for his private and family life, his home and his correspondence."[284] However, Article 8, section 2 permits interferences with this right to privacy when it is necessary:

> [I]n the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[285]

According to the European Court of Human Rights, whether a given infringement of privacy is permissible under Article 8, section 2 turns on whether it is proportional to the danger.[286]

Another example of the leading role of the EU with regard to data-protection law pertains to rules on how personal data collected by government authorities can be used and transferred. In *Bara v. CNAS & ANAF*, the European Court of Justice ruled that it is illegal to transfer personal data between different public institutions unless consent is given by the citizen whose data are to be

---

282. For example, Article 4 of the Inter-American Democratic Charter states, in part, that "freedom of expression and of the press are essential components of the exercise of democracy." 40 I.L.M. 1289, 1291 (2001).

283. International Covenant on Civil and Political Rights, art. 19, §§ 2–3, Mar. 23, 1976, 999 U.N.T.S. 171.

284. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8 ¶ 1, Sep. 3, 1953, 213 U.N.T.S. 221, 230 [hereinafter European Convention on Human Rights].

285. *Id.* art. 8(2).

286. *See* S. and Marper v. U.K., 1581 Eur. Ct. H.R. (2008) (deciding that retention of genetic data was disproportionate). Article 10 of the European Convention provides that, "Everyone has the right to respect for private life in relation to information about his or her health," thus arguably providing additional protection for health data. European Convention on Human Rights, *supra* note 284, art. 7.

transferred, and this individual is given prior notice of the transfer of information.[287] It remains to be seen, however, to what extent this ruling will effect initiatives, such as that by the Romanian government,[288] to create systems that aggregate personal information in a manner that would seem to make it easy to transfer individuals' personal information without consent or prior notice.

Much has been written about the extent to which these and other international and regional agreements protect communicative freedom, and it will not be replicated here. For present purposes, it suffices to say that these and other agreements provide moral, rhetorical, and at least arguable legal support for the protection of at least some anonymous speech. It is also clear that in the short run—say, the next decade—it would be unwise to rely on international agreements to solve the tensions caused by the forces ranged against anonymity. Nations with the strongest commitment to the rule of law may find domestic or international legal reasons to protect anonymous communications, but even in the United States with its strong First Amendment tradition and its record of directly relevant Supreme Court decisions, or in the EU with its world-leading data-protection regime, the protection of anonymous online communications in the face of its critics cannot be said to be settled. Furthermore, the reality is that, globally, the willingness of governments to respect international-human-rights commitments is anything but uniform, and tends to be at its least where it is needed most.

It seems, therefore, that political, pragmatic, and technical considerations are at least as likely to dominate the debate in the next decade as is anything else.

C. Pragmatic Considerations

Protecting anonymous speech is good policy for the world and good foreign relations for all democracies, even if high-profile events like the WikiLeaks document releases cause doubts in some quarters. The United States, the United Kingdom, and a small number of other democracies play a special role in internet communication because dissidents around the world rely on those democracies' servers to spread their messages.[289] More generally, it would be terribly unwise for the democratic nations that lead in software development and in provision of hosting services—broadly, the United States, Europe, and Japan—to engineer communications software and hardware in a way that can be abused to undermine them. Yet, as we have seen, the last decade has seen a substantial increase in the design and deployment of identification technologies.

The dangers of producing identification technologies, much less making them the default, are well illustrated by leaks that describe how the United States

---

287. Case C-201/14, Smaranda Bara & Others v. Preşedintele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF), ¶¶ 6, 15, (Oct. 1, 2015), http://curia.europa.eu.

288. *See supra* text accompanying notes 115–16.

289. TeleGeography Inc. has estimated that one-third of communications entering the United States is transit traffic with a destination outside that country. *See* Brown, *supra* note 128, at 102 (citing Barton Gellman et al., *Surveillance Net Yields Few Suspects*, WASH. POST (Feb. 5. 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/02/04/AR2006020401373.html).

provided technical assistance to several Latin American countries, including Panama and Paraguay, that sought to enhance their surveillance capabilities, even when the United States was aware, at least in the case of Panama, that these techniques likely would not be used in a manner consistent with the rule of law.[290] The Latin American governments claimed they needed the enhanced capabilities to fight terrorism or to conduct counter-narcotics operations, although the leaked cables show that the United States believed Panama at least "clearly made no distinction between legitimate security targets and political enemies."[291]

The availability of identification technologies attracts the attention of repressive regimes. Even if the technology remains in the United States, the United States' critical role in routing traffic risks creating an unfortunate temptation for a future Nixon or Kissinger—and, it must be said, the present-day Trump. A leader seeking to cozy up to a foreign government for some other purpose[292] may find it possible to slip that government information about their dissidents. Such an act might even be legal in the United States, because courts have generally held that foreigners abroad do not enjoy the protection of the U.S. Bill of Rights.[293]

And there is an even more important reason to resist efforts to make technologies of identification legally required. When we legislate communications architectures that have back doors, or front doors, or even spy holes for law enforcement, we create capabilities that create immediate dangers. If history is any guide, we will get it wrong, and create technical insecurities that will plague us all. But even if we get the technology just right, we create legal and moral problems. Perhaps we can trust our own commitment to the rule of law to protect us from too much abuse of these capabilities—or perhaps not. That debate is for another day, although that day may be upon us too soon. But we can be certain that when we design architectures of identification, what we require, or even what we standardize on, will without any doubt be exported to many other places including those where the commitment is to a different kind of law than that to which we aspire.

---

290. Rodriguez, *supra* note 137.

291. *Id.*

292. In this connection, consider Vladimir Frolov, *It Started with a Call: Presidents Trump and Putin Lay the Foundations of a New Partnership that Could Upend the Global Order*, MOSCOW TIMES (Jan 30, 2017), https://themoscowtimes.com/articles/the-new-bromance-56982 ("In this brave new world, Russia could be more important to Washington as a war ally, and Europe and NATO will have to compete against Russia for Washington's attention.").

293. *See, e.g.*, United States v. Verdugo-Urquidez, 494 U.S. 259, 270 (1990) (holding that the Fourth Amendment did not apply to the search by American authorities of the Mexican residence of a Mexican citizen and resident who had no voluntary attachment to the United States); Kleindienst v. Mandel, 408 U.S. 753, 762 (1972) (holding that the First Amendment rights of U.S. citizens do not require allowing noncitizen to visit the United States to foster debate).

More prosaic considerations also counsel caution. Rules that require government access to communications may solve some security problems, but they do so at the price of potentially creating new vulnerabilities.[294]

Similarly, rules that require internet users and others to identify themselves with their real names create new dangers of their own. In 2007, South Korea instituted regulations requiring that people use their real names and resident registration numbers when making online postings on websites with more than 100,000 visitors per day. A black market in stolen ID information soon flourished abroad, as Chinese and other internet users sought credentials that would allow them to play Korean games and participate on Korean social-networking sites.[295] Worse, the accumulated user data became a target for potential identity theft, a risk realized when someone stole data relating to about 35 million users of two popular South Korean websites, including their user IDs, passwords, resident-registration numbers, names, mobile-phone numbers, and email addresses. As a result of this theft, the South Korean government announced that it intended to abandon its real-name rules.[296]

And finally, there's simply the risk that identification becomes the new normal. Beginning March 1, 2015, China required all internet users to use their real names when registering accounts online. Styling the rule as a ban on impersonations, the Chinese government required ISPs to enforce the rules or face penalties.[297]

Whatever degree of credit the Internet and cell phones can or cannot claim for modern democratic uprisings, and there is debate on that question, there seems little reason to doubt that, as an ongoing matter, a regime bent on harassing dissent or limiting democracy finds, and as they become more ubiquitous will increasingly find, that the existence of identification technologies both inhibits dissent and makes punishing it more efficient. That is an outcome worth avoiding.

---

294. *See* HAL ABELSON ET AL., MASS. INST. TECH, COMPUTER SCI. & ARTIFICIAL INTELLIGENCE LAB. TECH. REPORT, PUB. NO. MIT-CSAIL-TR-2015-026, KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS (2015), http://dspace.mit.edu/handle/1721.1/97690; Declaration of Matt Blaze, Felton v. Recording Indus. Ass'n of Am., No. CV-01-2669 (D.N.J. 2001), http://www.crypto.com/papers/mab-feltendecl.txt ("Unfortunately, although some advances have been made in the use of rigorous mathematical techniques to prove and verify the security of some aspects of a system's design, there is not yet any systematic way to be sure that a proposed system or design will be secure in practice. Exploitable vulnerabilities are often discovered in proposed designs and in systems in actual use.").

295. *See Korean National ID Numbers Spring Up All Over Chinese Web*, KOREA HERALD (Aug. 3, 2011, 20:00), http://www.koreaherald.com/national/Detail.jsp?newsMLId=20110803000621.

296. Xinhua, *S. Korea Plans to Scrap Online Real-Name System*, CHINA DAILY http://www.chinadaily.com.cn/world/2011-08/11/content_13095102.htm (Aug. 11, 2011, 15:59).

297. *See China to Ban Online Impersonation Accounts, Enforce Real-Name Registration*, REUTERS (Feb. 4, 2015, 5:46 AM), http://www.reuters.com/article/2015/02/04/china-internet-censorship-idUSL4N0VE43Z20150204.

D. Defending Anonymous Communications

We seem likely to experience an expensive lesson in the costs of de-anonymization. Social media practices enable far more de-anonymization than most users suspect.[298] Attempts to legislate the identification of speakers and the keeping of records of their communications seem, at this writing, more likely to succeed than fail, both technologically and legally. Governments and industries around the world are constructing a surveillance infrastructure that is baked into standards, into hardware, into practices, and ultimately into expectations—a combination that likely will become ever more difficult to dislodge. Where once we believed that increases in computing power inevitably favored encryption over brute-force decryption,[299] now it seems as if governments are finding techniques, such as choke-point regulation, to make encryption less and less relevant to communications privacy.[300]

Nevertheless, there are counter-movements, ensuring a continued technological arms race between those who seek to enable long-distance private speech and those who wish to prevent it.[301] Probably the leading example is The Onion Router ("Tor") Project, which enables anonymous internet communication in a manner designed to protect against both eavesdropping and traffic analysis. Tor relies on a network of virtual tunnels designed to hide what any individual is doing by routing it through encrypted relays in a Tor network. Critically, no node in the relay ever knows the complete path that a data packet will take, and only the next-to-last-hop knows the ultimate destination. Although Tor does not directly provide anonymity, it disables many of the tools that might be used to identify a user.[302] On the other hand, while Tor seems to be effective, passing data along all

---

298. *See* JESSICA SU ET AL., DE-ANONYMIZING WEB BROWSING DATA WITH SOCIAL NETWORKS (forthcoming 2017), http://randomwalker.info/publications/browsing-history-deanonymization.pdf (reporting results of small test which demonstrated ability to de-anonymize 72% of users from web histories such as one might get from cookies or other online trackers).

299. *See, e.g.*, MATT BLAZE ET AL., MINIMAL KEY LENGTHS FOR SYMMETRIC CIPHERS TO PROVIDE ADEQUATE COMMERCIAL SECURITY 3 (1996), http://www.schneier.com/paper-keylength.pdf.

300. There are also technical hiccups. Consider, for example, the discovery that it is possible to identify speakers on encrypted VoIP communications. *See* L.A. Khan et al., *Speaker Recognition from Encrypted VoIP Communications*, 7 DIGITAL INVESTIGATION 65 (2009) (describing technique that "can correctly identify the actual speaker for 70–75% of the time among a group of 10 potential suspects").

301. Examples of anti-censorship technologies include "Speak to Tweet." *See Some Weekend Work that will (Hopefully) Enable More Egyptians to be Heard*, GOOGLE: OFFICIAL BLOG (Jan. 31, 2011), https://googleblog.blogspot.com/2011/01/some-weekend-work-that-will-hopefully.html ("[A]nyone can tweet by simply leaving a voicemail on one of the[] [provided] international phone numbers . . . and the service will instantly tweet the message . . . . No Internet connection is required.").

302. *See Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en (last visited Jan. 16, 2017).

those hops can impose a substantial toll on performance, although not as bad a toll as when it was new.[303]

Usage of Tor is growing rapidly. In January 2011, the Tor network advertised under ten gigabits per second ("Gb/s") of bandwidth, and users actually consumed even less. By March 2015, the Tor network advertised well over 120 Gb/s of bandwidth, and users consumed just over half of what was on offer.[304] Although there is no evidence that such an attack on the Tor network has yet occurred, Sarah Cortes suggests that a global web of Mutual Legal Assistance Treaties ("MLATs") could make it possible for a determined government to invoke those agreements to induce other governments to coordinate in performing traffic correlation and timing attacks on the Tor network sufficient to undermine the anonymity it seeks to establish.[305] The growing hostility to anonymity online suggests it will not be long before this or some other legal attack on Tor becomes a reality.

Alarmingly, in November 2015, the Tor Project accused the FBI of paying Carnegie Mellon University over $1 million to hack Tor users. The FBI initially denied the charge.[306] Court documents released in February 2016 suggest that it was in fact the Department of Defense, not the FBI, that funded the work,[307] but that the FBI was happy to use it.[308]

If the Tor network becomes unreliable, computer scientists will attempt to up the ante in the arms race between anonymizing technology and the law. One possible approach is a system called Telex, which promises to allow users to bypass internet censors:

> [W]e leverage censors' unwillingness to completely block day-to-day [i]nternet access. In effect, Telex converts innocuous,

---

303. *See* Jacob Appelbaum, *Over the Firewall and Into the Fire*, ADVOX (April 14, 2011, 3:35 PM), http://advocacy.globalvoicesonline.org/2011/04/14/over-the-firewall-and-into-the-fire/ (noting a 50% speed increase in Tor download times).

304. *Traffic*, TORMETRICS, https://metrics.torproject.org/bandwidth.html?graph=bandwidth&start=2011-01-19&end=2015-04-19 (last visited Jan. 16, 2017).

305. Sarah Cortes, *MLAT Jiu-Jitsu and Tor: Mutual Legal Assistance Treaties in Surveillance*, 22 RICH. J.L. & TECH. 2 (2015), http://jolt.richmond.edu/wp-content/uploads/Cortes-Publication-Version-PDF.pdf.

306. *See* arma, *Did the FBI Pay a University to Attack Tor Users?*, TOR (Nov. 11, 2015), https://blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users; Cyrus Farivar, *FBI: "The Allegation that We Paid CMU $1M to Hack into Tor is Inaccurate"*, ARS TECHNICA (Nov. 13, 2015, 1:42 PM), http://arstechnica.com/tech-policy/2015/11/fbi-the-allegation-that-we-paid-cmu-1m-to-hack-into-tor-is-inaccurate/; Andy Greenberg, *Tor Says Feds Paid Carnegie Mellon $1M to Help Unmask Users*, WIRED (Nov. 11, 2015, 5:01 PM), http://www.wired.com/2015/11/tor-says-feds-paid-carnegie-mellon-1m-to-help-unmask-users/.

307. *See* Alex Hern, *US Defence Department Funded Carnegie Mellon Research to Break Tor*, GUARDIAN (Feb. 25, 2016, 8:41 AM), http://www.theguardian.com/technology/2016/feb/25/us-defence-department-funding-carnegie-mellon-research-break-tor.

308. *See* Andy Greenberg, *FBI'S Tor Hack Shows the Risk of Subpoenas to Security Researchers*, WIRED (Feb. 25, 2016, 3:12 PM), http://www.wired.com/2016/02/fbis-tor-hack-shows-risk-subpoenas-security-researchers/.

> unblocked websites into proxies, without their explicit collaboration. We envision that friendly ISPs would deploy Telex stations on paths between censors' networks and popular, uncensored internet destinations. Telex stations would monitor seemingly innocuous flows for a special "tag" and transparently divert them to a forbidden website or service instead. We propose a new cryptographic scheme based on elliptic curves for tagging TLS handshakes such that the tag is visible to a Telex station but not to a censor.[309]

Telex is interesting because it stands incentives on their heads. Earlier attempts to give victims of censorship unedited access to the Internet required that they be able to make a connection to a computer located in a censorship-resistant jurisdiction. While that connection might be encrypted, it was in no way invisible and thus was vulnerable to detection and blockage. Telex, by contrast, is hidden in plain sight. The traffic to and from the end-user subjected to censorship or monitoring would appear to flow entirely to innocuous destinations, and would in effect be hijacked by third-party ISPs along the way without the knowledge of the persons running the innocuous ostensible target. If Telex were actually deployed (so far it is just a concept paper), the uncensored communications could be blocked only if the censors were willing to cut off access to the innocuous as well as the seditious—risking making the Internet useless domestically. Second, where normally one would think that deep packet inspection[310] was a threat to user privacy, Telex requires that complicit ISPs deploy the technology, as it is only by exploring the entire packet that the Telex-compliant intermediary will recognize a packet as one whose originator desires that it be hijacked.[311]

Another group calls itself "The Crypto Project" and promises to make available better encryption and anonymizing tools such as anonymous remailers.[312] Counter-surveillance plans and programs such as these serve to remind us that even though at this moment it seems that identification and surveillance have the

---

309. Eric Wustrow et al., *Telex: Anticensorship in the Network Infrastructure*, 20 PROC. USENIX SEC. SYMP. 30, 30 (2011), https://telex.cc/paper.html; *see also* Eric Wustrow et al., *Telex: Anticensorship in the Network Infrastructure*, USENIX, https://www.usenix.org/conference/usenix-security-11/telex-anticensorship-network-infrastructure (last visited Jan. 16, 2017) (presentation video).

310. "Deep packet inspection" refers to the examination of the full content of a communication—rather than just the headers—by an information intermediary such as an ISP. Typically, the automated examination searches for predetermined data sets or patterns. Among other things, deep packet inspection can give ISPs the ability to 'track' a user across websites. *See* JULIE S. BRILL, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 40 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

311. For a non-technical explanation of Telex's virtues, see James Grimmelmann, *Planet Telex*, LABORATORIUM (July 24, 2011, 2:46 AM), http://laboratorium.net/archive/2011/07/24/planet_telex.

312. *See About*, CRYPTO.IS, https://crypto.is/about (last visited Jan. 16, 2017); Dennis Fisher, *Behind the Scenes of The Crypto Project*, THREATPOST (Aug 30, 2011, 8:42 AM), https://threatpost.com/en_us/blogs/behind-scenes-crypto-project-083011.

upper hand, the outcome of this arms race is never certain except in one way: the fight will be expensive. In any case, who is ahead this year or next is almost beside the point. The decision as to how we shape social relations and relations between state and citizen ought not to turn solely, and in this case not even primarily, on what is technologically feasible. Just because we might be able to make anonymous communication impossible, or even just very, very difficult, does not mean that it is in our collective interest to do so.

There are those who say that in order to be safe we will have to create an infrastructure of mandatory identification. Some, including many of those charged with making decisions for the public's safety, clearly say it in the best of faith.[313] Others argue, sometimes despite the evidence,[314] that we in the United States must do so to protect the profits of an industry important to our trade balance. It is all very well for academics, often living in genteel surroundings, to ask that we not give in to fear, and to reply that before we create a regime that may be persistent and eventually ineradicable we should first ensure that there are no less restrictive means, and that we should consider all the externalities. But that is our job.

Here, then, are a few suggestions for avoiding what could otherwise be an outcome we likely will regret, also based on lessons learned from the past 20 years or so. Several of these concepts are already present in European-data-protection law, but none of them are legal requirements in the United States today:

- Demand evidence of the need for mandatory identification and data-retention rules, and insist the rules be proportional to the need.
- Avoid rules that lock technology into law.
- Always consider what an identification rule proposed for one purpose can do in the hands of despots.
- Control the exportation of identification technology to repressive regimes.
- Empower user self-regulation whenever possible rather than using choke-point regulation.
- Design filters and annotators before designing walls and takedown mechanisms.
- Require transparency. Make it an offense for devices to make records without clear, knowing, and meaningful consent on the part of the speaker, reader, listener, or viewer.
- Build alternatives in technology and law that allow people to control how much their counterparts know about them, and which by making selective release of information easier reduce the need for a binary choice between anonymity or data nudity.
- Require that privacy-enhancement be built in at the design level.

---

313. *See, e.g.*, STEWART BAKER, SKATING ON STILTS 226, 232–41, 314, 325–34 (2010).

314. *See* MEDIA PIRACY IN EMERGING ECONOMIES (Joe Karaganis ed., 2011), http://www.scribd.com/doc/50196972/MPEE-1-0-1 (debunking most of the claims that the content industry has made about the economics of third-world content privacy).

Those who disagree with these suggestions worry, with some reason, about new technology undermining the powers of states and sovereigns. Why is allowing people to speak freely to each other, without fear of eavesdroppers or retaliation, such a terrible thing? After all, most core government powers, like the power to tax, will not in fact be undermined in any substantial way by unfettered communication so long as we still need to eat and we want physical things such as houses.[315] The issues are the same "four horsemen" they have been for many years: fear of terrorism, money-laundering, child pornographers, and drug-dealers. In some countries, revolutionaries might be added as the fifth.

The flip side of these fears is the recognition that even if the power to speak freely and privately is sometimes misused, it is also empowering. Communicative freedom allows people to share ideas, to form groups, and to engage not just in self-realization, but in small-scale and even mass political organization.[316] Here then is the most important lesson to be learned, but one that needs to be learned over and over again: "Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical, minority views . . . . Anonymity is a shield from the tyranny of the majority."[317]

CONCLUSION

If it was not clear enough already, the results of the U.S. 2016 election should re-emphasize the importance of preserving not only the right to speak anonymously but also the practical ability do so. The Internet and related communications technologies have shown a great potential to empower end-users, but also to empower firms and especially governments at the end-users' expense. Governments (and firms) around the world have learned this lesson all too well, and are taking careful, thorough, and often coordinated steps to ensure that they will be among the winners when the bits settle. "Spying is cheap, and cheaper every day."[318] But only by preserving a space where we, and especially those individuals already burdened with repressive regimes, can speak anonymously—and thus freely—can we ensure that all of us will be among the winners in the ongoing battle between surveillance and freedom.

---

315. *See generally* Froomkin, *supra* note 32.

316. *See* David Kaye (Special Rapporteur on Freedom of Expression), U.N. Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, ¶ 56, U.N. Doc. A/HRC/29/32 (May 22, 2015), http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx ("56. Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity.").

317. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 335 (1995).

318. Cory Doctorow, *Technology Should Be Used to Create Social Mobility – Not to Spy on Citizens*, GUARDIAN (Mar. 10, 2015, 7:06 AM), http://www.theguardian.com/technology/2015/mar/10/nsa-gchq-technology-create-social-mobility-spy-on-citizens.