THE RISE AND FALL OF INVASIVE ISP SURVEILLANCE

*Paul Ohm**

Nothing in society poses as grave a threat to privacy as the Internet Service Provider (ISP). ISPs carry their users' conversations, secrets, relationships, acts, and omissions. Until the very recent past, they had left most of these alone because they had lacked the tools to spy invasively, but with recent advances in eavesdropping technology, they can now spy on people in unprecedented ways. Meanwhile, advertisers and copyright owners have been tempting ISPs to put their users' secrets up for sale, and judging from a recent flurry of reports, ISPs are giving in and experimenting with new forms of spying. This is only the leading edge of a coming storm of unprecedented and invasive ISP surveillance.

This Article seeks to help policymakers strike the proper balance between user privacy and ISP need. Policymakers cannot simply ban aggressive monitoring, because ISPs have legitimate reasons for scrutinizing communications on an Internet teeming with threats, so instead policymakers must learn to distinguish between an ISP's legitimate needs and mere desires.

In addition, this Article injects privacy into the network neutrality debate—a debate about who gets to control innovation on the Internet. Despite the thousands of pages that have already been written about the topic, nobody has recognized that we already enjoy mandatory network neutrality in the form of expansive wiretapping laws. The recognition of this idea will flip the status quo and reinvigorate a stagnant debate by introducing privacy and personal autonomy into a discussion that has only ever been about economics and innovation.

* Associate Professor of Law and Telecommunications, University of Colorado Law School. Versions of this article were presented to the Privacy Law Scholars 2008 Conference; Computers, Freedom, and Privacy '08 conference; and Telecommunications Policy Research Conference 2008. Thanks to Brad Bernthal, Aaron Burstein, Bruce Boyden, John Chapin, Samir Chopra, Danielle Citron, kc claffy, Will DeVries, Susan Friewald, Jon Garfunkel, Dale Hatfield, Stephen Henderson, Chris Hoofnagle, Orin Kerr, Derek Kiernan-Johnson, Scott Moss, Deirdre Mulligan, Frank Pasquale, Wendy Seltzer, Sherwin Siy, Dan Solove, Gerard Stegmaier, Peter Swire, Phil Weiser, Matt Yoder, and Tal Zarsky for their comments and suggestions.

TABLE OF CONTENTS

INTRODUCTION

Internet Service Providers (ISPs)[1] have the power to obliterate privacy online. Everything we say, hear, read, or do on the Internet first passes through ISP computers. If ISPs wanted, they could store it all, compiling a perfect transcript of our online lives.

In fact, nothing in society poses as grave a threat to privacy as the ISP, not even Google, a company whose privacy practices have received an inordinate amount of criticism and commentary.[2] Although Google collects a vast amount of personal information about its users, an ISP can always access even more because it owns and operates a privileged network bottleneck, the only point on the network that sits between a user and the rest of the Internet. Because of this fact about network design, a user cannot say anything to Google without saying it first to his ISP,[3] and an ISP can also hear everything a user says to any other websites like Facebook or eBay, things said that are unobtainable to Google. The potential threat to privacy from unchecked ISP surveillance surpasses every other threat online.

A potential threat to privacy, however, is not the same thing as a likely invasion, and to distinguish between the two we must make predictions about the future evolution of technology. In this case, the evidence points in opposite directions: on the one hand, historically, ISPs have respected user privacy.[4] On the other hand, evolving technology has cast aside hurdles that once prevented providers from monitoring invasively.[5]

A deeper look at the evidence shows a numbers of signs all pointing toward a coming wave of more surveillance: online wiretapping used to

1. This Article defines ISPs as the telecommunications companies that route communications to and from Internet-connected computers. The best-known ISPs are the cable companies that connect users through cable modems, such as Comcast, Cox, and Charter, and the telephone companies that connect users through digital subscriber line (DSL) connections, such as Verizon, AT&T, and Qwest. In addition, mobile carriers such as Verizon Wireless, Sprint Nextel, and AT&T Wireless are increasingly important ISPs. Lesser known ISPs serve institutional customers, providing Internet connectivity to companies, universities, and other ISPs. For a more detailed description of the various types of ISPs, see Part III.C.2.b.

2. *E.g.*, DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (2007); Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149 (2008); James Grimmelmann, *The Structure of Search Engine Law*, 93 IOWA L. REV. 1, 17–23, 39–41, 56–58 (2007).

3. There are a few exceptions, for example, when a user encrypts communications. These exceptions are discussed *infra* in Part I.D.1.c.

4. *See infra* Part II.B.1.

5. *See infra* Part I.A.3.

be easy, then it became difficult, and today it is easy again.[6] Easier wiretapping has made possible the disintegration of user privacy, while markets have accelerated the trend.[7] ISPs are desperately searching for new sources of revenue, and advertisers, technologists, and copyright owners are offering to supply that revenue in return for access to user secrets.[8]

Given this confluence of technological and economic forces, I foresee a coming storm of unprecedented, invasive ISP monitoring. If ISPs continue unabated, they will instigate the greatest reduction of user privacy in the history of the Internet, and users will suffer dire harms. Thus, the worst forms of ISP monitoring must be regulated.

To decrease the harms of ISP surveillance through regulation without unduly harming other things we value, we must engage in a cost-benefit balancing: what are the costs of additional regulation, and how do they compare to the net benefit to user privacy? To measure the benefits of regulation to reduce invasive ISP surveillance, I focus on the harm to individual users. ISP surveillance has and will continue to harm individuals, especially given the increasing invasiveness of the surveillance. Even if users have not experienced harms from yesterday's forms of ISP surveillance, we can make confident and well-supported predictions that they will suffer significant individual harm from today's and tomorrow's new forms of surveillance.

To measure the costs of regulating ISPs, I skeptically and critically evaluate arguments about the benefits of more ISP surveillance, arguing that security and necessity tend to be exaggerated, and focusing in particular on three often-heard defenses. First, ISPs oversell their ability to anonymize the data they collect to reduce potential harm. Second, providers claim the technical need to monitor user communications more deeply and thoroughly than they have in the past, but such claims do not hold up to close scrutiny. Third, ISPs claim that their users have consented to invasive surveillance, but these claims are tenuous.

In fact, Congress has already regulated ISP surveillance with the Electronic Communications Privacy Act (ECPA).[9] Although the ECPA likely prohibits many of these forms of ISP surveillance, because of some uncertainty in the meaning of the law, below I recommend a few amendments to clarify necessary protections.

Finally, the rise of invasive ISP surveillance invites connections to the network neutrality debate, a debate about who should control innovation on the Internet. In this Article, I connect the wiretapping laws to the network neutrality debate, something nobody else has done.[10] If pro-

6. *See infra* Part I.A.3.

7. LAWRENCE LESSIG, CODE: VERSION 2.0 50 (2006).

8. *See infra* Part I.A.2.d.

9. 18 U.S.C. §§ 2510–2712 (2006).

10. Although nobody has discussed the potential clash between wiretap laws and the net neutrality debate, Rob Frieden has discussed the mostly neglected privacy implications of the debate. *See generally* Rob Frieden, *Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and*

viders cannot scrutinize user communications closely—because of the wiretapping laws—they also cannot discriminate between different types of traffic. A private network is a more neutral network.

The Article proceeds in five parts. Part I offers a descriptive and predictive account of the threat to privacy posed by ISP surveillance, focusing in particular on the ever-changing history of network monitoring of the situation. Part II advances a better way to analyze privacy problems in dynamic, complex situations—one focused on well-grounded predictions about future harm and great skepticism about claims of the benefits of increased monitoring. Part III applies this analysis to the three defenses usually lodged in support of unfettered ISP network monitoring, demonstrating how each argument has been oversold. Finally, Parts IV and V compare the conclusions of this analysis to two features on the policy/regulatory landscape: the ECPA and the network neutrality debate.

I. PRIVACY ONLINE AND HOW IT IS LOST

Not a week seems to go by without the newspapers revealing a new form of invasive ISP monitoring.[11] These news stories paint a picture of an industry recently, suddenly, and sharply veering off of a long track record of respect for customer privacy.[12] This Part relates some of these developments and offers a few explanations for the sudden change.

These new forms of invasive ISP surveillance have harmed and will continue to harm users in significant ways, as also described below. This Part concludes by calling for a ban on at least the most invasive forms of ISP monitoring.

A. The Changing Nature of ISP Surveillance: Means, Motive, and Opportunity

This is a story of means, motive, and opportunity. An ISP's opportunity to invade user privacy stems from network architecture. The ISP operates the network chokepoint—its computers stand between the user and the rest of the Internet—and from this privileged vantage point it has access to all of its users' private communications. The motive to engage in invasive new forms of surveillance comes from many sources, but most importantly, from dire financial need. ISPs, to hear them tell it, are in an industry fighting for survival. In order to increase the revenues the in-

the Balance of Power Between Intellectual Property Creators and Consumers, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 633 (2008). Also, several non-academic commentators have explored similar points of view. Nate Anderson, *Deep Packet Inspection Meets 'Net Neutrality, CALEA*, ARS TECHNICA, July 25, 2007, http://arstechnica.com/articles/culture/Deep-packet-inspection-meets-net-neutrality.ars; Daniel Berniger, *Forget Neutrality—Keep Packets Private*, GIGAOM BLOG, Jan. 14, 2007, http://gigaom.com/2007/01/14/forget-neutrality-keep-packets-private/.

11. See *infra* Part I.B for a summary of recent stories.

12. *See infra* Part I.B.

dustry needs to survive, it would like to turn to new forms of moneymaking, most lucratively by selling user secrets for cash. Finally, ISPs only recently have acquired the means to engage in massive and invasive surveillance because surveillance tools have recently become much more powerful; online wiretapping used to be difficult and now it is easy, as demonstrated by a survey of the evolution of computer architecture.

1. Opportunity: Where the ISP Sits on the Network

An ISP controls a valuable and privileged bottleneck. It owns the point on the network between a user's computer and the rest of the Internet. Its principal role is routing—it receives communications from its users and sends them out to the rest of the world, and vice versa—and it performs this role by literally stringing cables between its facilities and each of its users' premises. This point on the worldwide map of the Internet, the ISP's connection to the end user, is a unique and critical point: the only point through which all of a user's communications must pass.

The chokepoint makes the ISP not only the single point of failure for the network, it makes it also the single greatest point of control and surveillance. It is no wonder that totalitarian regimes try to direct all Internet traffic through single, government-run network chokepoints, because they would like to be for all of their citizens what an ISP is for all of its users—the single best place to listen to (and stop, if need be) communications. Centralized control spawns surveillance power.

In the history of telecommunications law, ISPs are not the first entities with centralized access to all of a customer's communications; telephone companies control similar privileged points of access on the voice network. But, at least since Congress first regulated telephone wiretapping and up to the present day, telephone companies have respected subscriber privacy. Although telephone companies have always had surveillance capabilities, they have tended to listen to conversations only when they have been checking the line, investigating theft of services, assisting law enforcement, or after receiving the express, time-limited consent of those monitored.[13] Telephone companies caught recording in other circumstances have been punished severely for illegal wiretapping.[14]

At the same time, largely in line with federal legislation,[15] regulation,[16] and Supreme Court case law,[17] telephone companies have never

13. *See infra* Part IV.A.2.

14. *See infra* Part IV.A.1.

15. *Compare* 18 U.S.C. § 2511(1)(a) (2006) (subjecting those who intercept "any wire, oral, or electronic communication" to a felony prosecution and civil lawsuit), *with* § 3121(a) (subjecting those who use a "pen register . . . device" to a misdemeanor prosecution).

16. 47 C.F.R. § 64.2005 (2007) (permitting limited use for marketing of certain information relating to a customer's telephone services).

17. *Compare* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that the use of a pen register device did not constitute a Fourth Amendment search or seizure), *with* Berger v. New York, 388 U.S. 41, 58–60 (1967) (requiring heightened procedural requirements in order for the government to

hesitated to collect the non-content information relating to telephone calls: principally who called whom and for how long. Thus, the line between permissible and impermissible telephone monitoring has been drawn through the metaphor of the envelope, with "non-content addressing" information outside the envelope and open to scrutiny and the "content" enclosed within the envelope and off-limits.

Through a set of very important (mostly accidental) circumstances, our privacy online has ended up mirroring the kind of privacy we expect on the voice networks, or at least it had, up until a few years ago.[18] From the dawn of the commercial Internet in the mid-1990s until the very recent past, ISPs had respected user privacy, just as their telephone company forebears had, tracking communications in a broad way but not in a deep way.

ISPs have used two modes for monitoring user communications, one broad and noninvasive, the second narrow and invasive. First, ISPs deploy automated computer programs that scrutinize all of the communications—in Internet parlance, the packets—passing through critical points in a network, looking for troublesome communications and acting in response to concerns. Network providers conduct this kind of broad *automated monitoring* for five reasons: to gauge the health of the network, secure the network, detect spam, detect viruses, and police bandwidth.[19] Although automated monitors scan broadly, they are not very invasive because they are discriminating: they tend to ignore content and other information packed, to use another important metaphor, "deeply" within packets. They preserve privacy by keeping a shallow, limited view.

In contrast, ISPs turn to *targeted monitoring* to respond to incidents. When a network engineer suspects trouble on the network[20]—such as a suspected breach of network security by a hacker or unusually heavy congestion on the line—he will often switch on a targeted tool called a packet sniffer, which will peer deeply into packets and store everything it sees.

Compare the relative invasiveness of automated and targeted monitoring. Although targeted monitoring with a packet sniffer invades individual privacy much more than an automated monitor, a packet sniffer

obtain an order to wiretap), *and* Katz v. United States, 389 U.S. 347, 353 (1967) (prohibiting the use of a recording device to monitor telephone calls).

18. Jonathan Jacob Nadler, *The Impact of the FCC's New Broadband Regulation*, TELEPHONY ONLINE, Apr. 25, 2006, http://telephonyonline.com/regulatory/commentary/fcc_broadband_regulation_042506/ (stating that the FCC asserts a right to impose regulations on ISPs "that 'mirror' those traditionally imposed on telephone companies").

19. *Cf.* Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141, 166–67 (2003) (proposing network neutrality principle with six exceptions including protecting the network, limits on bandwidth usage, spam and virus delivery, quality of service, and security).

20. Targeted monitoring is often triggered by something an automated monitor has noticed. For example, an automated security monitor (such as a so-called intrusion detection system) might alert an operator of a suspected attack by a hacker.

rarely scrutinizes the data of many users, because it is usually deployed in the network where the information of only a few users can be seen and collected. Thus, automated monitoring protects privacy by "forgetting" much more than it remembers and targeted monitoring by being rare and temporary. Until things began to change not too long ago, most users, most of the time had been subjected only to automated, heavily filtered monitoring. Deep scrutiny was rare. Why did users once enjoy this much privacy, and what has changed?

2. Motive: Extraordinary Pressures

Shifting monetary incentives are the most important forces pushing toward greater ISP surveillance. ISPs have a great motive to pay a little more attention than they have before to their users' secrets. By doing so, they can tap new sources of revenue, which given their precarious situation, may be the only way they can guarantee their survival.

a. Pressure to Upgrade Infrastructure and Obtain ROI

ISPs are struggling for survival.[21] Many economists say the deck is stacked against them.[22] New Internet applications like virtual worlds and video delivery (in the form of YouTube clips, Hulu streams, and BitTorrent downloads) are bandwidth hungry and burden the existing infrastructure. Increasing bandwidth requires a huge capital investment and customers have been reluctant to pay more each month just for a faster connection.[23] The result, as one industry analyst puts it, is "accelerated erosion of the revenue per bit earned."[24]

Broadband ISPs have responded by searching for new sources of revenue. To this end, they have recognized the emerging market for what I call "trading user secrets for cash," which Google has proved can be a very lucrative market.[25]

21. Susan P. Crawford, *The Ambulance, the Squad Car & the Internet*, 21 BERKELEY TECH. L.J. 873, 877–78 (2006) (describing woes of telephone companies in part from competition from VoIP).

22. *See* DELOITTE TOUCHE TOHMATSU, TELECOMMUNICATIONS PREDICTIONS: TMT TRENDS 2007, at 7 (2007) ("Clearly, something has to change in the economics of Internet access, such that network operators and ISPs can continue to invest in new infrastructure and maintain service quality, and consumers can continue to enjoy the Internet as they know it today.").

23. Light Reading Insider, Deep Packet Inspection: Vendors Tap into New Markets, http://www.lightreading.com/insider/details.asp?sku_id=1974&skuitem_itemid=1060 (last visited Aug. 31, 2009).

24. *Id.*; *see also* DELOITTE TOUCHE TOHMATSU, *supra* note 22, at 7.

25. *See* DELOITTE TOUCHE TOHMATSU, *supra* note 22, at 7; Raymond McConville, *Telcos Show Their Google Envy*, LIGHT READING, Apr. 8, 2008, http://www.lightreading.com/document.asp?doc_id=150479.

b. Google Envy and the Pressure to Monetize

Providers have what some have called "Google envy."[26] Google has demonstrated how to grow rapidly by monetizing user behavior, in their case by displaying advertisements matching a users' recent search queries.[27] Google's success has redefined expectations for both profitability and privacy online. ISPs trying to replicate Google's performance eye the treasure trove of behavioral data—web transfers, e-mail messages, and instant messages—flowing through their networks, wondering if they can turn it into advertising money.

c. All-You-Can-Eat Contracts and Network Congestion

Another way ISPs might try to forestall the need to invest in expensive network upgrades is to reduce the use of the network. Some users and some applications cause a disproportionate amount of the network traffic, a byproduct of the fact that today ISPs sell service on an all-you-can-eat basis. If they wanted to, ISPs could identify the heaviest users without invading much user privacy by simply counting bytes on a per-user basis. They tend not to take this straightforward and privacy-respecting approach, however, because if ISPs were to cut-off heavy users altogether, they might lose customers and thus revenue.[28]

Instead, ISPs have realized that by invading privacy a bit more by tracking and blocking problem applications, they can free up bandwidth without barring any user from using the web and e-mail entirely.[29] Through this approach, ISPs can make a few users unhappy but not so unhappy that they will flee to a competitor.

d. Outside Pressures

Increasingly, third parties have exerted a great deal of pressure on ISPs to spy on their users. The recording and motion picture industries view ISP monitoring as an avenue for controlling what they see as rampant infringing activity, particularly on peer-to-peer networks.[30]

Government agencies want providers to assist in law enforcement and national security surveillance. In 1994, the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) successfully lobbied

26. McConville, *supra* note 25.

27. *Id.*

28. *Cf.* Peter Svensson, *Comcast Blocks Some Internet Traffic*, ASSOCIATED PRESS, Oct. 19, 2007, *available at* http://www.msnbc.msn.com/id/21376597 (stating that Comcast chose to limit access rather than cut off heavy users completely).

29. *Id.*

30. Anne Broache, *RIAA: No Need to Force ISPs by Law to Monitor Piracy*, CNET NEWS, Jan. 30, 2008, http://news.cnet.com/8301-10784_3-9861460-7.html (reporting Recording Industry Association of America's President Cary Sherman as "encouraged" to see that ISPs were experimenting with filtering technology).

Congress to enact the Communications Assistance for Law Enforcement Act (CALEA).[31] Under CALEA, providers are obligated to configure their networks to be able to quickly assist law enforcement monitoring.[32] Already saddled with the requirements of CALEA, providers may feel ongoing pressure to develop and deploy sophisticated network monitoring tools to help law enforcement stay ahead of surveillance challenges, perhaps out of a sense of civic obligation or to stave off future regulation.

Finally, many providers view new forms of network monitoring as a way to comply with Sarbanes-Oxley,[33] Graham-Leach-Bliley,[34] Health Insurance Portability and Accountability Act (HIPAA),[35] and recent e-discovery changes to the Federal Rules of Civil Procedure.[36] Vendors of monitoring products bolster these views by touting their deep-packet inspection (DPI) products as legal compliance tools.[37]

3. Opportunity: Evaporating Technological Constraints

Professor Lawrence Lessig has identified four regulators of online conduct—markets, norms, law, and technology.[38] Each of these has helped restrict the frequency and invasiveness of ISP monitoring, but technology has played an important role. Users have enjoyed privacy because the devices that monitor networks have been unable to keep up with the amount of data crossing networks.

Consider the simplest, most effective, and most privacy-invasive form of network monitoring imaginable: a packet sniffer that is always switched on, storing every packet crossing a network forever. I will return repeatedly to this possibility, which I call *complete monitoring*.

Even if ISPs have wished they could completely monitor, until very recently, they lacked the computing horsepower to analyze and capture information quickly enough to do so. ISPs have publicly conceded the limits of monitoring technology. For example, in response to calls from the copyright content industries to better police their networks, the British ISP Association complained, "ISPs are no more able to inspect and

31. Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended at 47 U.S.C. §§ 1001–1010 (2006)).

32. *Id.*

33. Pub. L. No. 107-204, 16 Stat. 745 (2002) (codified as amended in scattered sections of 18 U.S.C.).

34. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 15 U.S.C.).

35. Pub. L. No. 104-191, 100 Stat. 1936 (1996) (codified as amended in scattered sections of 29 U.S.C. & 42 U.S.C.).

36. *See* Letter from Chief Justice John Roberts to Representative J. Dennis Hastert, Speaker of the House (Apr. 12, 2006), http://www.supremecourtus.gov/orders/courtorders/frcv06p.pdf (transmitting the amendments to the Federal Rules of Civil Procedure that had been adopted by the Supreme Court of the United States pursuant to 28 U.S.C. § 2072).

37. CrossTec Corporation, Product Flyer for Activeworx Enterprise, http://www.activeworx.com/LinkClick.aspx?fileticket=6N3WtkLD5Ws%3D&tabid=122 (last visited Aug. 31, 2009) ("AE includes over 200 reports for Sarbanes-Oxley, HIPAA, PCI, GLBA and more.").

38. LESSIG, *supra* note 7, at 123.

filter every single packet passing across their network than the Post Office is able to open every envelope."[39] An executive for British Telecom concurred, "None of the technologies proposed by the ISPs to intercept or scan traffic as it travels across the network are proven to work at scale—the electronic equivalent of a 'stop and search' of all media files transmitted on our networks would not be a feasible solution."[40]

To better understand why the relative slowness of computers has constrained ISP surveillance, picture network monitoring like a police officer on the side of a road, scanning the passing traffic for drivers swerving or speeding or for cars with outdated license plates. How thoroughly the officer inspects the passing traffic depends on two metrics: the volume of traffic—the number of cars that pass by each hour—and the efficiency of the officer—how quickly he can inspect a single car. On the Internet, computers running monitoring tools are like the police officer and the rate of the network traffic flowing past the computer—the flow rate or bandwidth—is like the volume of cars passing on the highway.

Think about what happens to the officer on the side of the road over time. If we "upgrade" the police officer, by assigning him a partner, training him to work more quickly, or giving him scanning technology, he will be better able to keep up. On the other hand, if we upgrade the road, replacing a two-lane country path with a superhighway full of cars moving at top speed, the officer will probably falter. If we upgrade both the road and the officer, then success or failure depends on the relative rates of improvement.

The last scenario—of simultaneous improvement—describes network monitoring. Over the past twenty-five years both the speed of residential network connections and the power of monitoring hardware have significantly increased.[41] In the race between the fastest computer processors and the fastest residential network communications, the lead has changed hands twice, at very important historical junctures.[42]

a. Personal Computer to Pre-Commercial Internet

In 1984, users were already connecting personal computers, which were still in their infancy, to other computer modems, dialing bulletin board systems to chat with other users or transfer files.[43] At the time, the fastest consumer modem was the Hayes Smartmodem 1200, so named

39. British Broadcasting Corp., *Illegal Downloaders 'Face UK Ban*,' BBC NEWS, Feb. 12, 2008, http://news.bbc.co.uk/2/hi/business/7240234.stm (quoting the Internet Service Providers Association).

40. Eleanor Dallaway, *Music Piracy Born Out of a 'Something for Nothing' Society*, INFOSECURITY, Apr. 2008, at 17, 19.

41. *See infra* Part I.A.3.

42. *See infra* Part I.A.3.

43. *See generally* Jonathan Zittrain, *The Rise and Fall of Sysopdom*, 10 HARV. J.L. & TECH. 495 (1997) (describing the early days of online communities).

because it could send or receive 1200 bits of data per second.[44] At that rate, it would have taken nearly three hours to download the text of the Bible.[45]

Suppose the telephone company of 1984 had decided to monitor all of the digital bits traveling to and from all of its customers' computers over its lines. Imagine it had done this monitoring using personal computers, which in 1984 meant the brand new IBM PC AT, equipped with the Intel 80286 processor.[46] The 80286 could calculate 1.5 MIPS, or millions of instructions per second.[47] Assume for argument's sake that a processor needs twenty instructions to capture and store a single bit of modem data. A single PC AT, working at full capacity on this task, could wiretap 1,500,000 / (20 * 1200) = 62.5 Hayes Smartmodems. Because modems were so slow, the telephone company could monitor more than sixty users using a single personal computer without difficulty.[48] The police were dim witted, but they could keep up with the limited and pokey traffic on the road.

b. Dawn of the Commercial Internet

Let us jump ahead thirteen years. In 1997, customers began using cable modems to access the Internet[49] for the first time, enjoying an exponential gain in bandwidth to speeds approaching three megabits, or million bits per second.[50] At this rate, it would have taken only four seconds to download the Bible.[51]

Meanwhile, in 1997, Intel's fastest processor was the Pentium II, rated at 300 MIPS.[52] Thus, while connection speeds had increased ten thousand fold since 1983, processing power had increased only 200 times. Using the same back-of-the-envelope calculation, a Pentium II could monitor 300,000,000 / (20 * 3,000,000) = 5 cable modem connections.

44. Tony Messina, *Review—Hayes Smartmodem 1200*, ANALOG COMPUTING, June 1984, *available at* http://www.cyberroach.com/analog/an19/hayes_1200.htm.

45. The zip file version of the King James Bible downloadable from the Project Gutenberg archive measures 1.59 megabytes. The Bible, King James Version, Complete Contents, http://www.gutenberg.org/etext/7999 (last visited Aug. 31, 2009). 1,590,000 bytes x 8 bits per byte / 1200 bits per second = 10,600 seconds or 2.94 hours.

46. Old-Computers.com, *IBM PC AT*, http://www.old-computers.com/museum/computer.asp?c=185 (last visited Aug. 31, 2009).

47. Calisphere, *80286 Microprocessor Package, 1982*, http://content.cdlib.org/ark:/13030/kt7h4nc9c2/?layout=metadata&brand=calisphere (last visited Aug. 31, 2009).

48. This is almost certainly not literally true because of the back-of-the-envelope nature of the calculation. Most likely, the estimate of twenty instructions per bit copied is inaccurate; also, some other computing bottleneck may have limited monitoring long before a processor. The number is nevertheless useful to compare to the calculations from other eras that follow.

49. Lawrence J. Magid, *A Cable Modem Puts Surfer in the Fast Lane*, CNN, Oct. 16, 1997, http://www.cnn.com/TECH/9710/16/cable.modem.lat/index.html.

50. JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 136 (2005).

51. 1,590,000 bytes x 8 bits per byte / 3,000,000 bits per second = 4.24 seconds.

52. Marshall Brain, *How Microprocessors Work*, HOWSTUFFWORKS, http://computer.howstuffworks.com/microprocessor1.htm (last visited Aug. 31, 2009).

From the earliest days of the PC to the dawn of the commercial Internet, providers had become more than ten times less effective at monitoring their users. The smarter police were having trouble keeping up with the exponential increase in traffic flow.

Consider for another moment 1997, the year the cable modem made it much more difficult to wiretap users. In 1997, the Internet boom was in full swing, and users were logging on in unprecedented numbers.[53] Compared to the kind of users who had logged on in 1984, however, the 1997 users were less technically savvy and more ignorant of the informal etiquette that then governed the Internet.[54] Worse, there were too many new users to educate. Some called this the dawn of the "Eternal September," a wry reference to the previously only once-a-year influx of clueless college freshman that used to bedevil Internet veterans.[55]

Even worse, in 1997, malcontents—spammers and virus and worm authors—were attracted, like flies to honey, to the clueless hordes and their always-on broadband connections.[56] Providers must have feared these daunting new threats on the network, but because of the race they were losing between processing power and bandwidth, providers would have found it difficult to monitor the masses with ease.

According to our review of the history of the processor-bandwidth race, our privacy has *not* been selected out of a concern for user rights or to forestall regulation. Instead, in the mid-1990s, at the dawn of both the commercial Internet and the Eternal September, providers wanted to monitor invasively but had no choice but to monitor sparingly because they were losing an arms race.

c. The Present Day

Today, a decade after the dawn of cable modem, the Eternal September, and a massive increase in new threats, we are witnessing another order-of-magnitude bandwidth gain. Verizon now offers their FiOS fiber optic service to the home and already claims 1.8 million subscribers.[57] The fastest FiOS connection sold today delivers a blistering fifty megabits downstream.[58] Cable companies promise that a new kind of cable

53. *See* NUECHTERLEIN & WEISER, *supra* note 50, at 125 ("[T]he total number of Internet users . . . double[d] each year through the late 1990s.").

54. *See* Patricia Yevics, *Netiquette—What Is It and Why Should You Care?*, MD. ST. B. ASS'N BULL., Jan. 1999, http://www.msba.org/departments/loma/articles/officemngmt/netiquette.htm.

55. Eternal September was coined in 1993 when America Online first allowed its millions of users to have access to parts of the Internet. The Jargon File, September That Never Ended, http://www.catb.org/jargon/html/S/September-that-never-ended.html (last visited Aug. 31, 2009).

56. Susan Gregory Thomas, *Home Hackers*, U.S. NEWS & WORLD REP., Oct. 4, 1999, at 52 (noting how hacking of home computers had increased with spread of cable modems and DSL).

57. Brad Reed, *Verizon Expands 50Mbps FiOS Footprint*, NETWORK WORLD, June 19, 2008, http://www.networkworld.com/news/2008/061908-verizon-fios.html?hpg1=bn.

58. Eric Bangeman, *Verizon, Comcast Pump up the Bandwidth. Where's AT&T?*, ARS TECHNICA, May 10, 2007, http://arstechnica.com/news.ars/post/20070510-verizon-comcast-pump-up-

modem—based on a standard called DOCSIS 3.0—will deliver up to fifty megabits downstream as well.[59] Over such a connection, the Bible can be downloaded in about a quarter-of-a-second.[60]

Meanwhile, Intel's fastest consumer processor, the Core2Extreme, rates just shy of 30,000 MIPS.[61] Thus, despite the order of magnitude increase in bandwidth, processors have done much better than keep up, and providers today can monitor 30,000,000,000 / (20 * 50,000,000) = 30 FiOS connections, one-half the ratio they enjoyed between the PC AT and the Hayes Smartmodem in 1984 and six times the less favorable ratio of the late nineties.

d. The Future

The discussion thus far illuminates an interesting trend: high-bandwidth packet sniffing used to be easy, then it became very hard, and today it is easy again. The relative progress between bandwidth and processing power has see-sawed. But is this an oscillating pattern, and will bandwidth improvements outstrip processing power again in ten years? This is unlikely.

Moore's Law is a famous prediction about the computer chip manufacturing industry. Gordon Moore, the cofounder of Intel, predicted that innovation in his industry would continue to progress quickly enough that the maximum number of transistors that fit cheaply on a silicon microchip would double every two years.[62] Others claim the doubling occurs every eighteen months.[63] Roughly speaking, transistor density translates directly to computing power, so a processor with twice as many transistors will be twice as powerful and have twice the MIPS rating.

How does the growth in the rate of residential bandwidth compare? Two studies, one formal, one informal, suggest that the growth in the rate of residential bandwidth is similar to Moore's Law and perhaps a bit

the-bandwidth-wheres-att.html (claiming theoretical FiOS speeds up to 400 megabits after system upgrade).

59. *Id.* (noting DOCSIS 3.0 demonstration speed of 150 megabits); Brad Stone, *Comcast to Bring Speedier Internet to St. Paul*, N.Y. TIMES BITS BLOG, Apr. 2, 2008, http://bits.blogs.nytimes.com/2008/04/02/comcast-to-bring-speedier-internet-to-st-paul/.

60. 1,590,000 bytes x 8 bits per byte / 50,000,000 bits per second = 0.25 seconds.

61. Marco Chiappetta, *CPU's Core 2 "Extreme Machine*," COMPUTER POWER USER, Sept. 2006, at 64–66 (listing 27,051 MIPS for the "Dhrystone ALU" processor arithmetic measure). Like the traffic cop assigned a partner, today's chips not only work more quickly, but they can calculate multiple instructions in parallel using what are called multiple cores—essentially more than one processor on a single chip.

62. Moore's law traces back to a 1965 magazine article by Gordon Moore in *Electronics Magazine* in which he noted that the number of components that could be put on a microchip had been doubling each year. Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, ELECTRONICS, Apr. 19, 1965, http://download.intel.com/research/silicon/moorespaper.pdf ("The complexity for minimum component costs has increased at a rate of roughly a factor of two per year.").

63. *See* Tom R. Halfhill, *The Mythology of Moore's Law*, IEEE SOLID-STATE CIRCUITS SOC'Y NEWSL., Sept. 2006, at 21, 22, http://www.ieee.org/portal/cms_docs_societies/sscs/PrintEditions/200609.pdf (seeking to correct misconceptions about Moore's Law).

slower. In a paper from 1999, three analysts looked at historical modem technology and predicted that residential bandwidth to the Internet would grow at roughly the same rate as Moore's law.[64] At around that time, a web usability expert, Jakob Nielsen, predicted in 1998 that a high-end user's bandwidth grows 50 percent per year,[65] slower than the eighteen-month version of Moore's Law, leading him to conclude that "bandwidth grows slower than computer power."[66] These studies suggest that today's lead in processing power over networking will not diminish and may continue to widen.

If these predictions hold, then at least in the near term, ISPs will continue to have the advantage in the battle between speakers and sniffers. A technological constraint that used to protect privacy has since evaporated.

B. Signs of Change

Because ISPs have the means, thanks to recent advances in monitoring technology, motive—financial turmoil coupled with pressures to use new technologies to raise revenue and assist third parties—and opportunity—ownership of the network bottleneck—they have begun to embrace new forms of aggressive monitoring. In the past year in particular, the headlines have been filled with stories about ISPs conducting or proposing invasive new monitoring.[67] This has happened at a breathtaking pace and suggests an undeniable trend.

1. AT&T's Plans for Network Filtering

AT&T's executives have not been shy about their plans to begin monitoring their users in new ways. In 2007, reports emerged that AT&T was in talks with movie studios and record producers to develop new monitoring and blocking technologies.[68] In January 2008, during a panel discussion on digital piracy, when asked about the prospect of ISPs using "digital fingerprinting techniques on the network level," an AT&T

64. Charles A. Eldering et al., *Is There a Moore's Law for Bandwidth?*, IEEE COMM. MAG., Oct. 1999, at 117–21; *see also* Steven Cherry, *Edholm's Law of Bandwidth*, IEEE SPECTRUM, July 2004, at 58–60 (citing prediction of Hossein Eslambolchi, President of AT&T Labs, that telecommunications data rates are rising at exactly the same rate as Moore's Law).

65. Jakob Nielsen, *Nielsen's Law of Internet Bandwidth*, ALERTBOX, Apr. 5, 1998, http://www.useit.com/alertbox/980405.html.

66. *Id.* In 2000, George Gilder predicted that the total bandwidth of the entire network would double every three to four months. GEORGE GILDER, TELECOSM: HOW INFINITE BANDWIDTH WILL REVOLUTIONIZE OUR WORLD 11 (2000). This prediction inspired Gilder to speculate about a world of infinite bandwidth. Note that Gilder's measurement factors in the number of users connected online, which may explain why it is so much faster than the rates recited in the text. *Id.* at 10.

67. *See, e.g.*, *infra* notes 68–93 and accompanying text.

68. Peter Burrows, *AT&T to Get Tough on Piracy*, BUS. WK., Nov. 7, 2007, http://www.businessweek.com/technology/content/nov2007/tc2007116_145984.htm (reporting that AT&T, NBC, and Disney had invested a combined $10 million in a company called Vobile, which develops a content recognition system).

senior vice president said, "We are very interested in a technology based solution and we think a network-based solution is the optimal way to approach this."[69] Later that month, AT&T CEO Randall Stevenson confirmed that the company was evaluating whether to undertake this kind of monitoring.[70]

In 2008, AT&T entered into a new collaboration called Arts + Labs headed by Michael McCurry, the former press secretary under President Clinton, and Mark McKinnon, former media adviser to the younger President Bush.[71] Although the mission of the collaboration is still a bit unclear, one can make educated guesses based on the identities of the collaborators, which also include Microsoft; several copyrighted content owning companies like Viacom, NBC, and Universal; and Cisco, the world's leading vendor of networking hardware.[72] What all of these parties hold in common is an interest in increased ISP filtering, and McCurry has admitted that the group would try to prevent Congress from enacting new laws prohibiting ISPs from blocking copyrighted material.[73]

2. Phorm

A company called Phorm markets a plan for a new method of providing targeted Internet marketing.[74] British ISPs British Telecomm, Carphone Warehouse, and Virgin Media reportedly plan to work with Phorm to target ads based on a user's Web surfing habits.[75] By reconfiguring the ISPs' servers, Phorm will be able to access, analyze, and categorize websites users have visited into separate advertising channels.[76] If a user visits many travel-related websites, she will begin to see more travel-related ads at Phorm-affiliated websites.[77] Virasb Vahidi, Phorm's COO, has bragged, "As you browse, we're able to categorize all of your Internet actions. We actually can see the entire Internet."[78]

Because these ads will target to behavior, consumers will be more likely to click on them, justifying higher advertising rates and earning

69. Brad Stone, *AT&T and Other I.S.P.'s May Be Getting Ready to Filter*, N.Y. TIMES BITS BLOG, Jan. 8, 2008, http://bits.blogs.nytimes.com/2008/01/08/att-and-other-isps-may-be-getting-ready-to-filter/.

70. Tim Barker, *AT&T's Idea to Monitor Net Creates Web of Suspicion*, ST. LOUIS POST-DISPATCH, Feb. 13, 2008, at A1 (stating further that "[t]he company has since clarified its position, saying it does not plan to play the role of Internet cop").

71. Saul Hansell, *Hollywood Wants Internet Providers to Block Copyrighted Files*, N.Y. TIMES BITS BLOG, Sept. 25, 2008, http://bits.blogs.nytimes.com/2008/09/25/hollywood-tries-to-get-support-for-having-isps-block-copyrighted-files/.

72. *Id.*

73. *Id.*

74. Louise Story, *A Company Promises the Deepest Data Mining Yet*, N.Y. TIMES, Mar. 20, 2008, at C3.

75. *Id.*

76. RICHARD CLAYTON, THE PHORM "WEBWISE" SYSTEM 11 (May 18, 2008), http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf.

77. *Id.*

78. Story, *supra* note 74.

more money for Phorm, the ISP, and the website hosting the ad. The potential earnings might be significant; some have suggested that British Telecomm alone will earn eighty-seven million pounds per year from its proposed deal with Phorm.[79]

When Phorm's business model was revealed, it inspired a fury of commentary and criticism in the UK. The Information Commissioner, an office sponsored by the UK Ministry of Justice,[80] assessed the program and concluded, in part, that their analysis "strongly supports the view that Phorm products will have to operate on an opt in basis."[81] Professor Ross Anderson, an expert in security engineering, said, "The message has to be this: if you care about your privacy, do not use BT, Virgin or Talk-Talk as your internet provider."[82] In response to this type of criticism and government scrutiny, some of Phorm's ISP partners have decided to require customers who want Phorm-targeted ads to opt in.[83]

3. Charter Communications and NebuAd

In May 2008, Charter Communications announced its own plan to partner with a company called NebuAd, which sells an advertising model very similar to Phorm's.[84] Charter's Senior Vice President sent a letter to customers informing them of the plan and giving them instructions on how to opt out.[85]

Like its industry peers, Charter was criticized following its announcement. The public advocacy groups Free Press and Public Knowledge hired a technical consultant to produce a report dissecting NebuAd's methods.[86] Congressmen Edward Markey and Joe Barton wrote a letter to Charter's CEO arguing that the plan might violate federal law and urging the company not to act until it had consulted with Congress.[87]

79. Charles Arthur, *TalkTalk to Make Phorm Use Opt-In, Not Opt-Out*, GUARDIAN, Mar. 10, 2008, http://www.guardian.co.uk/technology/blog/2008/mar/10/talktalktomakephormuseopt; *see also* discussion *infra* Part I.B.3.

80. Information Commissioner's Office, Who We Are, http://www.ico.gov.uk/about_us/who_we_are.aspx (last visited Aug. 31, 2009).

81. INFO. COMM'RS OFFICE, PHORM—WEBWISE AND OPEN INTERNET EXCHANGE 2 (2008), http://msl1.mit.edu/furdlog/docs/2008-04-08_uk_ico_phorm_finding.pdf.

82. Jim Armitage, *Web Users Angry at ISPs' Spyware Tie-Up*, EVENING STANDARD, Mar. 6, 2008, http://www.thisismoney.co.uk/bargains-and-rip-offs/broadband-and-phones/article.html.

83. British Broadcasting Corp., *Users Offered Ad Tracking Choice*, BBC NEWS, Mar. 11, 2008, http://news.bbc.co.uk/1/hi/technology/7289481.stm.

84. There may be some technical differences under the hood. For example, Phorm sends bogus "redirect" error messages to a Web browser in order to send traffic through a Phorm-run server, CLAYTON, *supra* note 76, at 3, whereas NebuAd injects code into a user's Web browsing stream. ROBERT M. TOPOLSKI, NEBUAD AND PARTNER ISPS: WIRETAPPING, FORGERY AND BROWSER HIJACKING 2 (2008), http://www.freepress.net/files/NebuAd_Report.pdf.

85. Letter from Joe Stackhouse, Senior Vice President, Customer Operations, Charter Commc'ns (May 14, 2008), http://graphics8.nytimes.com/packages/pdf/technology/20080514_charter_letter.pdf.

86. *E.g.*, TOPOLSKI, *supra* note 84.

87. Letter from Rep. Edward J. Markey, Chairman, Subcomm. on Telecomms. and the Internet, and Joe Barton, Ranking Member, H. Comm. on Energy and Commerce, to Mr. Neil Smit, President

The Senate Subcommittee on Interstate Commerce, Trade, and Tourism held a hearing about interactive advertising prompted by the controversy.[88] Connecticut's Attorney General also released a letter urging Charter not to implement the program.[89] In the face of this criticism, about a month after announcing the plan, Charter abandoned it.[90] In the meantime, NebuAd has partnered with other, smaller ISPs, some of which have already implemented the program.[91] In November 2008, six ISPs and NebuAd were sued by fifteen of their customers seeking to represent a class action of tens of thousands of customers for alleged violation of state and federal privacy laws.[92]

4. Comcast Throttles BitTorrent

In August 2007, subscribers to Comcast's cable Internet service began having trouble transferring files using the BitTorrent peer-to-peer protocol.[93] Although BitTorrent users had long suspected that ISPs had been slowing down particular types of Internet traffic, Comcast's techniques seemed more aggressive and harder to evade.[94] Eventually, the techniques were confirmed by the press[95] and activists[96] and the Federal Communications Commission (FCC) opened an investigation.[97] Throughout the ensuing firestorm, Comcast has repeatedly defended its actions as necessary steps to manage its network.[98]

---

and CEO of Charter Commc'ns (May 16, 2008), http://markey.house.gov/docs/telecomm/letter_charter_comm_privacy.pdf.

88. Wendy Davis, *Senate Slates Online Ad Hearing, Microsoft Set to Testify*, ONLINE MEDIA DAILY, June 12, 2008, http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticleHomePage&art_aid=84513.

89. Jim Salter, *Charter Drops Web Tracking Plans*, ASSOCIATED PRESS, June 25, 2008, *available at* http://www.msnbc.msn.com/id/25368034.

90. *See* Saul Hansell, *Charter Suspends Plan to Sell Customer Data to Advertisers*, N.Y. TIMES BITS BLOG, June 24, 2008, http://bits.blogs.nytimes.com/2008/06/24/charter-suspends-plan-to-sell-customer-data-to-advertisers/.

91. *See, e.g.*, TOPOLSKI, *supra* note 84; Stephanie Clifford, *Web Privacy on the Radar in Congress*, N.Y. TIMES, Aug. 11, 2008, at C1.

92. Paul Elias, *Web Tracker NebuAd Sued over Privacy Claims*, ASSOCIATED PRESS, Nov. 14, 2008, *available at* http://www.usatoday.com/tech/products/2008-11-13-2070037456_x.htm.

93. Ernesto, *Comcast Throttles BitTorrent Traffic, Seeding Impossible*, TORRENTFREAK, Aug. 17, 2007, http://torrentfreak.com/comcast-throttles-bittorrent-traffic-seeding-impossible/ (first public posting related to controversy).

94. *Id.*

95. Svensson, *supra* note 28.

96. Seth Schoen, *EFF Tests Agree with AP: Comcast Is Forging Packets to Interfere with User Traffic*, ELECTRONIC FRONTIER FOUND., Oct. 19, 2007, http://www.eff.org/deeplinks/2007/10/eff-tests-agree-ap-comcast-forging-packets-to-interfere.

97. Associated Press, *F.C.C. to Look at Complaints Comcast Interferes with Net*, N.Y. TIMES, Jan. 9, 2008, at C4.

98. *E.g.*, Letter from Kathryn A. Zachem, Vice President, Reg. Aff., Comcast Corp. to Marlene H. Dortch, Sec'y, FCC, at 6 (July 10, 2008), http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6520033822 ("[T]he current network management technique implemented by Comcast was reasonable in light of available technology . . . .").

Although this practice has become the center of attention in the network neutrality debate, it is only tangentially about privacy. Although Comcast, by definition, had to monitor user communications in search of BitTorrent packets, what alarmed people most was the way Comcast had handled BitTorrent packets. Its computers would masquerade as the computer on the other end of the communication, sending a forged RST, or "reset," packet, causing the user's computer to think that the network connection had failed.[99] After reports of this behavior emerged, the FCC launched an investigation[100] and held two hearings.[101]

In response to the public firestorm and regulator scrutiny, in March 2008, Comcast entered into an agreement with the vendor BitTorrent, the company founded by the inventor of the BitTorrent protocol.[102] Under the agreement, Comcast promised it would change its network management approach, controlling network use in a "protocol agnostic" manner, but not until the end of the year.[103] Specifically, Comcast now plans to manage traffic based on bandwidth usage rather than application choice.[104]

On August 1, 2008, the FCC, in an unprecedented and landmark ruling, concluded that Comcast had "unduly interfered with Internet users' rights" and ordered the company to end its discriminatory practices, disclose more details about its practices, and disclose details about its replacement practices.[105] Comcast has appealed the ruling.[106]

C. Forecast

I predict that ISPs, faced with changes in technology and extraordinary pressures to increase revenues, will continue aggressively to expand network monitoring. The AT&T, Comcast, Charter, NebuAd, and Phorm examples will prove not to be outliers, but the first steps in a steady expansion of industry practices. Unless some force—regulatory or non-regulatory—intervenes, the inevitable result will be ISPs conducting full-packet capture of everything their users do, supposedly with their users' consent.

99. Ernesto, *supra* note 93.

100. Associated Press, *supra* note 97.

101. Ryan Kim, *Net Neutrality Debate Leads to Stanford*, S.F. CHRON., Apr. 18, 2008, at D1; Stephen Labaton, *F.C.C. Weighing Limits on Slowing Web Traffic*, N.Y. TIMES, Feb. 26, 2008, at C3.

102. Press Release, Comcast, Comcast and BitTorrent Form Collaboration to Address Network Management, Network Architecture and Content Distribution (Mar. 27, 2008), *available at* http://www.comcast.com/About/PressRelease/PressReleaseDetail.ashx?PRID=740.

103. *Id.*

104. Vishesh Kumar, *Comcast, BitTorrent to Work Together on Network Traffic*, WALL ST. J., Mar. 27, 2008, at B7 (quoting Tony Warner, Chief Technology Officer at Comcast).

105. Press Release, FCC, Commission Orders Comcast to End Discriminatory Network Management Practices (Aug. 1, 2008), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-284286A1.pdf.

106. *See* John Dunbar, *Comcast to Appeal FCC Web Traffic Ruling*, SEATTLE TIMES, Sept. 4, 2008, http://seattletimes.nwsource.com/html/businesstechnology/2008158470_webfcc04.html.

As further proof of this trend, consider the rise of the DPI industry.[107] These companies sell hardware and software tools that consume packets voraciously, like packet sniffers, but monitor at all times, whether or not the ISP has specific cause.[108] According to a report from the *Light Reading Insider*, a Telecom industry trade publication, the market for DPI tools has broadened in the past year.[109] Sales of DPI products in 2007 reached $400 million and are expected to rise to one billion dollars in 2010.[110]

The vendors in this new submarket are not shy about the impact their tools have on privacy. Solera Networks, a vendor of DPI devices, trumpets the loss of privacy: "See EVERYTHING on the network. With a complete historical record, there are no more secrets; every action taken on the network is recorded and stored. You can go back in time to watch network breaches, slow hacks, and network slowdowns unfold."[111] Another vendor, Endace, uses the motto, "power to see all."[112]

The "power to see all" will eviscerate user privacy. Let us now look closely at the privacy interests implicated.

D. Measuring and Comparing the Harms of Complete Monitoring

Significant increases in ISP surveillance would not matter, however, without proof of harm. How is anybody harmed by packet sniffing and deep packet inspection, and are the harms vague and abstract or specific and concrete? For now, let us take the worst case scenario—complete monitoring. How are customers harmed when ISPs begin capturing every single inbound and outbound packet traversing their networks? How does this threat compare to threats to privacy raised by other entities—online and offline—that have been the subject of much more prior commentary and regulation? Admittedly, because this question focuses on the worst-case scenario, even if we conclude that complete monitoring will significantly harm customers, we must analyze how that potential harm will change with less-than-complete monitoring, a topic considered in Part II.

To assess the harm caused by ISP deep packet inspection, we must first understand how much information an ISP can access and compare

107. *Cf.* Wu, *supra* note 19, at 163 (predicting future restrictions providers might impose on network neutrality by surveying "the marketing efforts of equipment vendors who target the cable and DSL market").

108. *Cf. id.* at 163–64.

109. Light Reading Insider, *supra* note 23.

110. Kyle, *Deep Packet Inspection: Vendors Tap into New Markets*, DPACKET.ORG, Nov. 28, 2007, https://www.dpacket.org/articles/deep-packet-inspection-vendors-tap-new-markets (summarizing Light Reading report).

111. Solera Networks, Top 10 Reasons for Complete Network Visibility, http://www.soleranetworks.com/solutions/top-ten.php (last visited Aug. 31, 2009).

112. Endace, http://www.endace.com/ (last visited Aug. 31, 2009).

that to the amount of information accessible by other entities that may threaten privacy.

1. Measuring What ISPs Can See

How much personal information flows through an ISP's wires and is stored on its computers? In modern connected life, almost no other entity can access as much personal information.

a. Visual Privacy as a Metaphor for Online Privacy

We first need a way to discuss—qualitatively if not quantitatively—how much privacy an entity can invade. Visual privacy is a useful analog to online communications privacy. Just as privacy in the real world can be invaded by visual observation, so too can privacy in the virtual world be violated by packet observation.

For example, the nature and magnitude of a visual invasion depends on at least two things: the vantage point of the observer—is he situated across the street, inside my home, or on a satellite 30,000 feet in the air?—and on his viewing technology—is he using the naked eye, binoculars, a telescope, or a thermal imager? Similarly, our online privacy varies based on the observer's vantage point—is he running code on my computer, sitting at an upstream spot on the network, or watching the log files of the websites I visit?—and the tools he wields—is he using packet sniffers, spyware, or cookies?

Moreover, with visual privacy, we tend to think of breadth and depth of view. The naked eye, for example, views broadly but shallowly: it can view an entire landscape, but it cannot make out details in far away things. Binoculars or telescopes, on the other hand, provide fine detail of distant objects, but fixate on a narrow part of the landscape.

b. What ISPs Can See

Because the ISP is the gateway—the first hop—to the Internet, almost any communication sent to anybody online is accessible first by the ISP. Like the naked eye, ISPs can view our online activity across the Internet landscape, seeing everything we do regardless of destination or application. In fact, no other online entity can watch every one of a user's activities, making the ISP's viewpoint uniquely broad. In addition, like a telescope, ISPs can view our activity deeply, because packet sniffers can store everything.

Imagine that an ISP conducts complete monitoring on one user for one month. The data stored comprises a complete transcript of everything the user has done on the Internet for the month. It includes a replica copy of every web page visited and every e-mail message sent or re-

ceived. It includes every instant message, video download, tweet, book update, file transfer, VoIP conversation, and more.

c. What ISPs Cannot See: Encrypted Contents and Use of Another ISP

An ISP's broad and deep visual field is marred by two blind spots. First, ISPs cannot see the communications of users using a different provider. Many people surf the web in different places, perhaps at home, work, and increasingly, on their mobile phones. An ISP can obviously not see the packets sent through another provider, so unlike Google, which can associate behavior at each of these three connections to the same unique login ID, the residential ISP cannot. Still, given the amount of time people spend online, even if a typical user splits her browsing into three equal parts, each part will still contain a significant amount of personal information.[113]

Second, an ISP cannot decipher encrypted communications. For example, when a user visits a website protected by the Secure Sockets Layer (SSL) protocol (signified by the little lock icon in the user's browser) all of the content sent between the user and website is surrounded by a tunnel of encryption. If a user visits Gmail using SSL, an ISP cannot read his e-mail messages.[114]

The encryption blind spot exception does not swallow the rule of broad vision for at least two reasons. First, most users and websites do not use encryption because it is difficult and expensive to implement[115] and slows the user's browsing experience.[116] Gmail, for example, disables SSL by default and sends communications "in the clear" instead.[117] Second, even though ISPs cannot read encrypted messages, they can use so-called traffic analysis techniques to reveal some personal information

113. Nielsen reports that the average American Internet user spends twenty-seven hours online per month. NIELSEN, A2/M2 THREE SCREEN REPORT 4th Quarter 2008, at 2 tbl.2 (2009), http://www.nielsen-online.com/downloads/3_Screens_4Q08_final.pdf.

114. Chris Sogohian, *Avoiding the NSA Through Gmail*, SLIGHT PARANOIA BLOG, Feb. 3, 2007, http://paranoia.dubfire.net/2007/01/avoiding-nsa-through-gmail.html (discussing Gmail and SSL, noting that SSL is turned off by default).

115. SSL requires the use of an SSL certificate, and although some of these are available for free, obtaining one from a reputable vendor can be expensive. *See* DOUG ADDISON, WEB SITE COOKBOOK 206 (2006) ("SSL certificates are not cheap, and they must be renewed every year or two.").

116. According to the Official Gmail blog:

> We use https [which indicates a website protected by the SSL protocol] to protect your password every time you log into Gmail, but we don't use https once you're in your mail unless you ask for it (by visiting https://mail.google.com rather than http://mail.google.com). Why not? Because the downside is that https can make your mail slower. Your computer has to do extra work to decrypt all that data, and encrypted data doesn't travel across the internet as efficiently as unencrypted data. That's why we leave the choice up to you.

Ariel Rideout, *Making Security Easier*, THE OFFICIAL GMAIL BLOG, July 24, 2008, http://gmailblog.blogspot.com/2008/07/making-security-easier.html.

117. *Id.*

from encrypted data streams.[118] Some have alleged that Comcast has been able to detect and throttle encrypted BitTorrent packets masquerading as something else.[119]

2. *Comparing ISPs to Other Entities*

One way to make claims about the invasiveness of complete monitoring by an ISP is to compare it to other claimed threats to privacy, including both online and offline threats.

a. ISPs Compared to Google

How does the amount of information accessible to an ISP compare with the amount of information accessible to Google, a company often scrutinized for its privacy practices?[120] Today, Google has archived more information about an individual user's behavior than almost any other entity on earth. But virtually everything Google knows about a user is also accessible to his or her ISP. For example, Google stores a user's search queries, which over time can amount to a complete intellectual profile of that user.[121] These search queries can be sniffed by ISPs, and both Phorm and NebuAd specifically ferret out Google search queries from user packets.[122]

Likewise, the ISP can scrutinize communications sent to almost all of Google's other services. Every time a user adds an appointment to his Google Calendar, sends or receives an e-mail message through Gmail, reads blogs using Google Reader, edits a word processing document in Google Docs, or views a video in Google-owned YouTube, his computer sends copies of his messages, requests, and behavior first through his ISP.[123]

118. For example, Italian researchers have demonstrated a method they call a "tunnel hunter," which can be "trained" to distinguish the ordinary use of an encrypted protocol called ssh from the use of other protocols masquerading as ssh. Maurizio Dusi et al., *Detection of Encrypted Tunnels Across Network Boundaries*, IEEE Int'l Conf. on Comm., May 2008, at 1738.

By raising the specter of a sophisticated ISP attack, this might be an example of the Myth of the Superuser I have condemned elsewhere. Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1327 (2008). Then again, ISPs have the motivation, tools, know-how, and resources to conduct sophisticated monitoring. This fact counteracts, at least somewhat, the usually completely unsupported use of the Myth.

119. Ernesto, *supra* note 93.

120. Saul Hansell has been reporting extensively about Google's privacy track record for the *New York Times*. *E.g.*, Saul Hansell, *Peeking into Google's Use of Data*, N.Y. TIMES BITS BLOG, July 30, 2008, http://bits.blogs.nytimes.com/2008/07/30/peeking-into-googles-use-of-data/; Saul Hansell, *I.P. Address: Partially Personal Information*, N.Y. TIMES BITS BLOG, Feb. 24, 2008, http://bits.blogs.nytimes.com/2008/02/24/ip-address-partially-personal-information/.

121. *See* Grimmelmann, *supra* note 2, at 18.

122. CLAYTON, *supra* note 76, para. 46, 56–57, at 6, 7 (describing Phorm's use of search terms); TOPOLSKI, *supra* note 84, at 6 (describing NebuAd's interception of Google data).

123. *Cf.* Humphrey Cheung, *Point and Click Gmail Hacking at Black Hat*, TG DAILY, Aug. 2, 2007, http://www.tgdaily.com/content/view/33207/108/ (describing use of sniffer to grab Gmail cookies, allowing the attacker to access the user's inbox).

Thus, an ISP can access all of the information available to Google about their shared customers.[124] It follows that anything that can be said about Google's threat to privacy can also be said about the threat posed by an ISP. But this is only a small slice of the ISP's information pie, as an ISP can also access communications sent to and from Yahoo!, Microsoft, AOL, MySpace, Facebook, eBay, Wikipedia, Amazon, and Craigslist, as well as the millions of websites unaffiliated with any of these giants. The ISP's potential invasion of privacy is the sum of the risk to privacy of every other website on the web.

Google cannot dream of building the same type of digital dossier that an ISP can, unless a user chooses to use Google for everything he does online.[125] Google cannot know what users buy on Amazon or eBay, what they read on the *New York Times*, or who they friend on Facebook. An ISP can. Furthermore, Google can never know what a user does or says when he uses non-web Internet applications such as instant messaging or VoIP telephony. An ISP can.

b. ISPs Compared to Google Plus DoubleClick

Google's threat to privacy increased significantly with its acquisition of Internet advertising giant DoubleClick. DoubleClick is the intermediary, the middle man that matches advertisers with websites, bringing users the banner and pop-up advertisements they see every day.[126]

Many privacy advocates fret about DoubleClick because it can track the movement of users across different websites.[127] For example, using a technology called a third-party cookie, DoubleClick can know that the user who just clicked on a Nintendo ad at Nickelodeon's nick.com is using the same computer as the person who had previously clicked on a Sony ad while surfing at AOL.com.[128] They might even be the same person.

Because DoubleClick can correlate information about user behavior across thousands of websites, in a sense, DoubleClick poses a similar

124. Of course, it would take some time for an ISP to catch up to Google's previously collected mountain of data. Google claims to store data for eighteen months, a number chosen in negotiations with European privacy officials. Nate Anderson, *Google Bows to EU Pressure, Will Anonymize Log Files After 18 Months, Not 24*, June 13, 2007, ARS TECHNICA, http://arstechnica.com/tech-policy/news/2007/06/google-bows-to-eu-pressure-will-anonymize-log-files-after-18-months-not-24.ars. So, it might take a year and a half from the time ISPs flip the switch saving everything until they surpass Google's collection.

125. As time passes, the possibility that a user could do this becomes more likely. Google's stated purpose is to "organize the world's information." What started as a search company has expanded to provide (at least) dozens of different services. JOHN BATELLE, THE SEARCH 248–50 (2005); *see also* Google, More Google Products, http://www.google.com/intl/en/options/ (last visited Aug. 31, 2009).

126. DoubleClick.com, About Us, http://www.doubleclick.com/about/about_us.aspx (last visited Aug. 31, 2009).

127. Courtney Macavinta, *Privacy Fears Raised by DoubleClick Database Plans*, CNET NEWS, Jan. 25, 2000, http://news.cnet.com/2100-1023-236092.html.

128. Opentracker, *All About (Third Party) Cookies*, http://www.opentracker.net/en/articles/all-about-cookies-third-party.jsp.

threat to the one posed by an ISP. In reality, DoubleClick's view is much narrower than an ISPs both in depth and breadth. An ISP can see much more deeply than DoubleClick because it can peer into the content of the packet. DoubleClick, in contrast, knows little more than that a particular user downloaded a particular ad while visiting a particular page. Other content displayed on that page can be seen by the ISP and not by DoubleClick.

More importantly, ISPs can see a much broader swath of the Internet than DoubleClick. DoubleClick can only see activity at its clients' websites. According to one analyst, "DoubleClick has relationships with thousands of large Web publishers."[129] Although this is impressive, according to studies there are tens of millions of active websites in the world,[130] the overwhelming majority of which are not DoubleClick customers. In contrast, your ISP can view information about any website on the Internet as soon as you choose to visit it.

Even summing the threat from Google and DoubleClick presents less concern than the threat from ISP surveillance. This sum is no greater than the parts, and the parts taken together are still much less than the threat from ISPs.

c. ISPs Compared to Spyware Distributors

Although Google and DoubleClick cannot threaten privacy as much as an ISP can, there is an entity with access to as much private information, at least for some users: the spyware distributor. The term spyware has many meanings,[131] but it generally describes a class of computer programs that infect a user's computer usually without consent, monitor many of the user's activities, and periodically "phone home," sending information about the user's habits and communications to a third party.[132]

Spyware can rival and might even surpass a packet sniffer-wielding ISP. Spyware, for example, can collect email as it is being drafted, stor-

129. David Hallerman, *Google: Tomorrow the World?*, EMARKETER, Apr. 16, 2007, http://www.emarketer.com/Article.aspx?id=1004812.

130. Netcraft, June 2009 Web Server Survey, http://news.netcraft.com/archives/web_server_survey.html (last visited Aug. 31, 2009) (showing 240 million hostnames in use with 73 million active websites in June 2009).

131. *See* H.R. REP. NO. 109-32, at 10 (2005) (report of Committee on Energy and Commerce, noting that "[t]he Committee received testimony that spyware represents a range of software programs on a broad continuum from the most pernicious criminal activities on one end to the less threatening but still intrusive on the opposite end of the spectrum"); FED. TRADE COMM., STAFF REPORT, MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE 3 (Mar. 2005) ("Panelists generally agreed that reaching an industry consensus on one definition [of spyware] has been elusive because of the technical complexity and dynamic nature of software.").

132. Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283, 1298 (2005). Spyware uses a variety of surveillance techniques. For example, a so-called keylogger will record every key depressed on the keyboard, thus recording e-mail, search queries, and passwords as they are entered. *Id.*

ing messages that are later deleted, capturing the typos and later-discarded paragraphs. Spyware can even work while a computer is offline, phoning home whenever it detects a network. Spyware can capture traffic sent through more than one ISP, and it can even capture messages before they are encrypted.

On the other hand, spyware usually has much less breadth than an ISP's complete monitoring. A spyware distributor needs to infect a computer before he can watch it; an ISP can watch every customer whenever it wants. Although some studies suggest that nearly 90 percent of computers are infected with spyware,[133] these computers are probably infected with many different forms of spyware and phone home to many different watchers;[134] no single spyware distributor has access to information about every infected computer.

Ultimately, whether complete monitoring is more invasive or less invasive than spyware is a close call. The two surveillance methods have much in common, and others have compared aggressive new forms of ISP surveillance to spyware.[135] Both NebuAd and Phorm have hired former spyware employees.[136] The fact that they are comparable to one another supports calls to regulate complete monitoring, because many states have already banned or otherwise limited spyware.[137]

133. For example, a 2004 study found that 80 percent of survey respondents had spyware installed on their computers. Cynthia L. Webb, *Invasion of the Data Snatchers*, WASH. POST, Oct. 25, 2004, http://www.washingtonpost.com/wp-dyn/articles/A60881-2004Oct25.html. Another study performed by antispyware company Webroot found spyware on 89 percent of consumer PCs. Webroot Software Inc., State of Spyware Q2 2006, http://www.webroot.com/resources/stateofspyware/excerpt.html (last visited Aug. 31, 2009).

134. One imprecise way to measure the number of hosts visible by any one distributor is to look at the size of so-called botnets. Botnets are networks of infected computers that can be controlled from one central source. John Markoff, *Attack of the Zombie Computers Is a Growing Threat, Experts Say*, N.Y. TIMES, Jan. 7, 2007, at 1. According to some experts, the largest botnets contain around 400,000 infected victims. Dan Goodin, *Kraken Stripped of World's Largest Botnet Crown (Maybe)*, THE REGISTER, Apr. 9, 2008, http://www.theregister.co.uk/2008/04/09/kraken_disagreement/. Although this is a large number it is much smaller than the customer population of the largest ISPs. AT&T and Comcast each serve more than 14 million high-speed Internet customers. Comcast, Corporate Overview, http://www.comcast.com/corporate/about/pressroom/corporateoverview/corporateoverview.html (last visited Aug. 31, 2009); AT&T, 2007 AT&T Accomplishments, http://www.att.com/Common/files/pdf/att_accomplishments_2007.pdf.

135. Alex Goldman, *ISPs Behaving Like Spyware*, ISP PLANET, Apr. 23, 2008, http://blog.ispplanet.com/blog/2008/04/isps-behaving-like-spyware.html; Joseph Menn, *NebuAd Hires Like Spyware, Acts Like Spyware*, L.A. TIMES TECH. BLOG, June 20, 2008, http://latimesblogs.latimes.com/technology/2008/06/nebuad-hires-li.html; Posting of Dan to N.Y. TIMES BITS BLOG, http://bits.blogs.nytimes.com/2008/09/08/dealing-with-isp-snooping/#comment-33000 (Sept. 8, 2008, 15:21 EST) ("Phorm or other Deep Packet Inspection is Adware or Spyware ON YOUR NETWORK . . . .").

136. Menn, *supra* note 135 ("At least five high-ranking employees at NebuAd . . . are veterans of one of the more notorious spyware companies around, Claria Corp."); Chris Williams, *ISP Data Deal with Former 'Spyware' Boss Triggers Privacy Fears*, THE REGISTER, Feb. 25, 2007, http://www.theregister.co.uk/2008/02/25/phorm_isp_advertising/ ("Phorm is run by Kent Ertegrul . . . [whose] most notable [previous] foray online was as the founder of PeopleOnPage, an ad network that operated earlier in the decade and which was blacklisted as spyware by the likes of Symantec and F-Secure.").

137. Susan P. Crawford, *First Do No Harm: The Problem of Spyware*, 20 BERKELEY TECH. L.J. 1433, 1437–45 (surveying state spyware laws).

d. ISPs Compared to Offline Entities

As people migrate more of their traditionally offline activities onto the Internet, the amount and sensitivity of information an ISP can possess will come to outweigh the data owned by offline entities, even those traditionally thought to pose the greatest risks to privacy. Doctors, lawyers, and therapists all possess the kind of information society treats as among the most sensitive, yet today well-connected people routinely reveal the same kind of highly protected information they would have once only told these three types of professionals when communicating online.

Someone with an embarrassing medical condition, for example, would probably rank her medical records as the records whose possible breach poses the single-greatest threat to her privacy. Google and Microsoft have recently launched services designed to warehouse medical records online, thus putting ISPs in a position to access this information in transit too.[138] A person with a shameful family secret or a history of some sort of scornful conduct will worry today most about breaches by his family members or by witnesses to the conduct, but secrets increasingly get whispered in e-mail or instant message; and much scornful conduct—say the collection of child pornography—has a way of flourishing online.

Finally, it nearly goes without saying that ISPs can possess much more information than the offline entities that Congress has chosen to regulate as threats to privacy. For example, drivers' license records,[139] records held by financial institutions,[140] educational records,[141] and video viewing records[142] are all restricted from certain types of disclosure, use, or collection under federal law. What is contained in these databases pales in comparison to what an ISP can access.

E. Harms

How are people harmed, inconvenienced, or otherwise troubled when ISPs completely monitor? The potential inconvenience, embarrassment, hardship, or pain that could result from the trove of data of complete monitoring is limited only by the wickedness of one's imagination. Friendships can be ruined, jobs can be lost, and reputations can be destroyed. Any person who has ever been undone by a fact about him or

138. The risk is ameliorated because Microsoft and Google both use mandatory SSL for their health records services.

139. Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 108 Stat. 2099 (codified as amended at 18 U.S.C. §§ 2721–2725 (2006)).

140. Right to Financial Privacy Act, Pub. L. No. 95-630, 92 Stat. 3641 (1978) (codified as amended at 12 U.S.C. §§ 3401–3420 (2006)).

141. Education Amendments of 1974, Pub. L. No. 93-380, 88 Stat. 44 (codified as amended at 20 U.S.C. § 1232g (2006)).

142. Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified as amended at 18 U.S.C. §§ 2710–2711 (2006)).

herself could have suffered the same fate in modern times at the hands of an ISP with a packet sniffer.

It is not just things uttered that are put at risk, because the ISP will also be able to compile a detailed record of thoughts and behavior as well.[143] An ISP can track your ailments, emotions, and the state of your relationships. It can learn your travel plans, big dates, and trips across town to do mundane chores. It can know how often you call your mother, e-mail your sister, or send gifts to your grandfather. It can know what you read, watch, buy, and borrow. And unlike Google, it already has an authoritative record of your home address, because it sends your bill there each month, and very likely your credit card and bank account numbers as well.

It is not only the user who is watched whose privacy is implicated because. As Justice Brandeis put it, "The tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him."[144] Moreover, ISPs can track what third parties say about a person, even when he or she is not a party to the communication.

And it can do all of this effortlessly. The all-knowing digital dossiers compiled by data brokers that Professor Solove has written about at least take some effort and expense to assemble.[145] Data brokers need to buy and mine data, requiring money, technology, and human capital. An ISP needs to do none of this. It simply flips a virtual switch and waits. And the data it collects is not limited to the things in a user's digital dossier like financial data and government-obtained data; it contains all of this and more.

Of course, none of these harms materialize from the storage of information alone. ISPs that completely monitor will promise to use the data for well-specified purposes, keeping the data under lock-and-key at other times. If perfect security could be guaranteed, we would worry much less about the risk of harm. Perfect security is impossible, however, and the risk of internal misuse—from bored employees for example—can probably never be extinguished.[146]

143. Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1269 (2004) (stating that electronic surveillance "records behavior, social interaction, and everything that a person says or does").

144. Olmstead v. United States, 277 U.S. 438, 476 (1928) (Brandeis, J., dissenting).

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

146. There are many reported cases of bored or curious employees browsing the records of celebrities. Glenn Kessler, *Celebrity Passport Records Popular*, WASH. POST, July 4, 2008, at A1 (passport records); Charles Ornstein, *Hospital to Punish Snooping on Spears*, L.A. TIMES, Mar. 15, 2008, at A1 (hospital records); Andrea Coombes, *IRS Employee Sentenced for Snooping*, MARKETWATCH, Aug. 20, 2008, http://www.marketwatch.com/news/story/irs-worker-snooped-tax-records-of-almost-200-celebrities (tax records); Ryan J. Foley, *Workers Snooping on Customer Data Common*, ASSOCIATED PRESS, Feb. 23, 2008, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/02/23/national/a044051597.DTL&hw=privacy+database&sn=001&sc=1000 (public utility records); Amol Sharma, *Obama's Cellphone Account Breached by Verizon Employees*, WALL ST. J., Nov. 21, 2008,

The trove of data can also be exposed to external threats. Collections of web surfing data would be a prime target for theft and a devastating risk for loss. Providers will, of course, promise security, but there will inevitably be breaches.

Moreover, these databases full of ISP-collected information will prove irresistible to civil litigants armed with subpoenas.[147] In the past year, a court ordered YouTube to produce to Viacom the viewing records for every public video ever hosted on its site;[148] another court ordered a website that had intentionally declined to log data about visitors for privacy's sake to turn on logging to reveal potential copyright infringers;[149] and the DOJ, in a civil case, subpoenaed search engine query archives from Yahoo!, Microsoft, and Google.[150]

Much recent privacy scholarship has tried to provide theoretical accounts of the potential harms of information privacy breaches.[151] These scholars have, for example, identified potential harms to autonomy, freedom, human relationships, equality, and even democracy and civil society. Because the data flowing through an ISP's veins is as "diverse as human thought,"[152] and encompasses every kind of public and private, sensitive and benign human relationship and action, every single harm identified by scholars is raised by the specter of ISP monitoring. These harms will be considered in greater depth in Part II, but for now, consider one specific harm especially triggered by ISP surveillance: the dismantling of online boundaries. Professor Julie Cohen describes the benefits of psychological repose, which can be undermined from surveillance.[153] She talks about how "[t]he injury . . . does not lie in the exposure of formerly private behaviors to public view, but the dissolution of the boundaries that insulate different spheres of behavior from one another."[154]

http://online.wsj.com/article/SB122724536331647671.html (reporting unauthorized browsing of then President-Elect Barack Obama's cell phone records by Verizon employees).

147. Saul Hansell, *One Subpoena Is All It Takes to Reveal Your Online Life*, N.Y. TIMES BITS BLOG, July 7, 2008, http://bits.blogs.nytimes.com/07/07/the-privacy-risk-from-the-courts/ ("[I]n the United States, one of the biggest privacy issues is what information about people can be revealed through a court process, either as part of a criminal investigation or in some sort of civil dispute.").

148. Miguel Helft, *Google Told to Turn Over User Data of YouTube*, N.Y. TIMES, July 4, 2008, at C1.

149. Columbia Pictures Indus. v. Bunnell, No. CV06-1093, 2007 WL 2080419, at *1 (C.D. Cal. May 29, 2007) (Order Granting in Part and Denying in Part Plaintiffs' Motion to Require Defendants to Preserve and Produce Server Log Data and for Evidentiary Sanctions and Denying Defendants' Requests for Attorneys' Fees and Costs), http://www.eff.org/files/filenode/torrentspy/columbia_v_bunnell_magistrate_order.pdf; Electronic Frontier Foundation, Columbia v. Bunnell, http://www.eff.org/cases/columbia-pictures-industries-v-bunnell (last visited Aug. 31, 2009) (discussing order).

150. Verne Kopytoff, *Google Must Reveal Some Secrets: Judge Rules in Case Involving Internet Privacy but Has Concerns About Divulging Too Much*, S.F. CHRON., Mar. 15, 2006, at C1.

151. *See infra* Part II.A.

152. Reno v. ACLU, 521 U.S. 844, 852 (1997) (quoting district court findings of fact, 929 F. Supp. 824, 842 (E.D. Pa 1996)).

153. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425 (2000).

154. *Id.*

The dismantling of boundaries is one of the worst effects of pervasive ISP monitoring. Today, we enjoy very little privacy about where we go *on a particular site* (or family of sites) from the watchful eye of the owner of that site, and we know it, but we also know that the site owner cannot "follow" us when we leave his site. There are boundaries the owner cannot cross. Even unsophisticated users probably have a sense of this, understanding that the *New York Times* tracks which articles we read on its site but has no way of knowing what we do when we visit the *Washington Post*.[155] These expectations are breached once ISPs begin monitoring, giving us the impression that we are always watched. According to Cohen, "[p]ervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream."[156] We will lose, in her terms, "the expression of eccentric individuality."[157]

The question of harm has often bedeviled privacy scholars.[158] Too often, privacy harms are inchoate, seemingly minor, and hard to articulate. Not so with ISP monitoring, which raises the risk of terrifying, nearly boundless harm.

F. Conclusion: We Must Prohibit Complete Monitoring

In sum, given the potential for terrifying privacy breaches and the evidence that the constraints protecting users from such breaches have fallen, a law should ban ISP complete monitoring. Although much work—descriptive, predictive, and normative—has already been done, the hardest steps lay ahead. Thus far, this Article has analyzed only the worst case—the risks from complete monitoring. The more difficult and important question is how much other conduct—conduct that invades less privacy than complete monitoring—should policymakers regulate?

II. WEIGHING PRIVACY

In Part IV, this Article summarizes the federal and state wiretapping laws that already provide privacy protection from many forms of ISP monitoring. Providers will likely be sued or prosecuted under these laws if they continue crossing the lines they have recently crossed.[159] Before analyzing those laws, let us start with a blank slate and ask: What

155. This is why third-party cookies, which allow one advertiser to follow our behavior across other sites that have contracts with the advertiser, cause alarm. But third-party cookies are easy to block and they reveal nothing to websites who do not deal with the third-party advertiser. When ISPs monitor, it is often hard if not impossible to opt-out, and there are no limits to the scope of their surveillance.

156. Cohen, *supra* note 153, at 1426.

157. *Id.*

158. *See, e.g.*, Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 768–72 (2007).

159. *See supra* note 92 and accompanying text (describing lawsuit against NebuAd).

principles *should* underlie an ideal regulation of ISP monitoring, given the complexity of balancing privacy with an ISP's legitimate needs? The Article approaches this difficult task first in this Part by surveying and critiquing earlier approaches to balancing communications privacy. Although this Article proposes no new theory, it improves on the work of others, refining a much more workable approach to weighing privacy. Then, Part III applies this new approach to offer an ideal ISP monitoring regulation.

A. Theories of Information Privacy

As Professor Daniel Solove puts it, privacy "is a concept in disarray."[160] Nearly everybody celebrates its value, at least as a general matter, but many have grown frustrated trying to define it, despairing at the term's vagueness and breadth.[161]

As a way out of this morass, Professor Solove, a self-avowed pragmatist who traces an intellectual lineage directly back to John Dewey,[162] recommends a four-pronged approach for setting out theories of privacy,[163] most of which I adopt here. First, he eschews searches for "rigid conceptual boundaries and common denominators" in favor of a Wittgensteinian "family resemblances" approach.[164] In other words, he recommends a pluralistic (as opposed to unitary), empirical approach to conceptualizing privacy. "Privacy is not one thing, but a cluster of many distinct yet related things."[165] Second, Solove advises that privacy should be discussed neither too specifically nor too generally.[166] Solove says that we should simultaneously "resolve privacy issues by looking to the specific context,"[167] while at the same time use "a general framework to identify privacy harms or problems and to understand why they are problematic."[168] Third, he embraces a dynamic view of privacy, because notions of privacy change over time and place.[169] Finally, he advocates a focus on problems instead of preferences, expectations, or types of information as his organizing principle.[170]

Solove thus provides a pragmatist's frame for developing theories of privacy in *Understanding Privacy*, but he offers less in this work about the content of such theories. In other work, Solove seems to embrace a consequentialist balancing, weighing the benefits against the harms of in-

160. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008).
161. *See id.*
162. *Id.* at 47–49.
163. *Id.* at 40–41.
164. *Id.* at 42–44.
165. *Id.* at 40.
166. *Id.* at 46–49.
167. *Id.* at 48.
168. *Id.* at 49.
169. *Id.* at 50–51.
170. *Id.* at 74–77.

vading privacy.[171] Most theorists embrace the same methodology, offering refinements for how to measure benefits and harm.[172]

Instead of reconceptualizing privacy, I follow the same essential structure of earlier scholars. But by focusing on ISP surveillance, I can offer a refinement to their work. When assessing the privacy of dynamic, rapidly changing technologies, one should take a serious look—an engineer's look—at the dynamics of the problem.

B. Analyzing Privacy in Dynamic Situations

Harms to privacy can be measured in two ways—by focusing solely on past problems or by speculating about potential future harm. Solove's third prong encourages a dynamic, future-looking analysis, but this is hard to do well, because there is a risk of regulating based on idle speculation, science fiction, or just-so stories about what is possible.[173] For the most part, policymakers should focus on past examples of harm, but they should not ignore undeniable indicators of future harm, so long as they measure them in a careful, empirically sound way.

To assess profoundly dynamic situations—those in which events break weekly, as in the ISP surveillance situation—I propose a three-step process for assessing the likelihood of future significant harm to privacy. First, and most importantly, how sensitive is the private information at risk? If the answer is "not very sensitive," then the threat of potential future harm is small and the analysis can end. This step measures the worst case scenario. In the case of ISPs, we should look at the amount and type of information revealed by complete monitoring.

When highly sensitive private information is at risk, we must next assess the historical record: have there been harmful breaches of privacy in the past? If the answer to the question is yes, the need for regulation is likely significant. If the answer is no, then, in step three, policymakers should make predictions about the future. This is the trickiest part, and policymakers need to base their predictions on a careful, rigorous assessment of the situation. Because at this stage in the analysis there has been no evidence of significant past harm, there should be a presumption that potential future harm is unlikely. The first step of the process was addressed in Part I; because ISPs possess a vast—uniquely vast—potential data reach, the analysis must continue.

171. *See* Solove, *supra* note 158.

172. AMITAI ETZIONI, THE LIMITS OF PRIVACY 196 (1999); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 968 (1989).

173. I have critiqued the harmful effects of speculation and science fiction in an earlier work. *See* Ohm, *supra* note 118, at 1330.

1. ISPs Have a Track Record of Respecting Privacy

The second step is to see if ISPs have abused their potential power. Despite the potential harms an ISP could cause, there are few examples of past breaches. No reported cases to date have discussed the liability of an ISP for unlawfully running packet sniffers, except for lawsuits against providers for supporting government monitoring.[174] Telephone companies and their employees are sued and criminally charged more often than ISPs, usually for installing devices like pen registers, which record telephone numbers dialed from a phone, and even occasionally for recording voice conversations in the pursuit of telephone service thieves.[175] Some of these cases will be discussed in greater depth in Part IV, but for now it is enough to note that many of these providers were vindicated because they were trying to track abusers of their systems.[176]

Even news accounts about ISPs collecting information were once rare. This is an amazingly pristine track record, especially when compared to lawsuits and news reports about other types of online entities being careless with personal information.[177]

2. Constraints—and Signs of Evaporation

The analysis thus far has raised contradictory signals. On the one hand, ISPs threaten privacy more than almost any other institution in society. On the other hand, despite this potential to do harm, ISPs have a good track record for respecting privacy. The tie-breaker is the overwhelming evidence of change developed earlier.[178] There are convincing reasons to suspect that providers have respected privacy only because they have been constrained from doing more; however, technological barriers to extensive monitoring have fallen significantly.

Many scholars have recently focused on the role of code as a regulator of online conduct.[179] To adapt an argument from Professor Harry Surden, the limits of ISP monitoring technology have guaranteed users a

174. Electronic Frontier Found., Hepting v. AT&T, http://www.eff.org/cases/hepting (last visited Aug. 31, 2009) (collecting materials relating to lawsuit against AT&T for assisting NSA monitoring program).

175. United States v. Pervaz, 118 F.3d 1, 1–3 (1st Cir. 1997); United States v. Mullins, 992 F.2d 1472, 1474–75 (9th Cir. 1993); United States v. McLaren, 957 F. Supp. 215, 216 (M.D. Fla. 1997); Sistok v. Nw. Tel. Sys., Inc., 615 P.2d 176, 178–79 (Mont. 1980).

176. *See, e.g.*, *Pervaz*, 118 F.3d at 6; *McLaren*, 957 F. Supp. at 219–20.

177. *E.g.*, Ellen Nakashima, *AOL Takes Down Site with Users' Search Data*, WASH. POST, Aug. 8, 2006, at D1 (describing release of AOL search queries); Joseph Pereira, *How Credit-Card Data Went Out Wireless Door*, WALL ST. J., May 4, 2007, at A1 (describing loss by TJX Cos. of tens of millions of credit card numbers); Dep't of Justice, *Former Officer of Internet Company Sentenced in Case of Massive Data Theft from Acxiom Corporation*, Feb. 22, 2006, http://www.usdoj.gov/criminal/cybercrime/levineSent.htm (describing conviction and sentence of hacker who stole data from Acxiom Corp.).

178. *See supra* Part I.B.

179. *See, e.g.*, LAWRENCE LESSIG, CODE (1999); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 555 (1998); Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 682 (2003).

structural constraint right in privacy.[180] Structural rights promise privacy not by a regulator's edict, but through technology and architecture.[181] But in this case, the constraint right has been recently breached. Surden argues that as latent constraint privacy rights evaporate, policymakers should consider reinstituting those rights by enacting laws.[182]

In addition to changes in technology, the recent news stories about Comcast, AT&T, Phorm, and Charter prove that markets and norms have failed to prevent new breaches.[183] If only one of these stories had emerged, we might have dismissed it as the overreaching of a bad actor. But when so many different large players in such a short period of time have begun to diverge from past practice and have been accused by others of breaching informal norms, and when an entire industry—the DPI industry—of more invasive monitoring techniques has arisen, we need to ask if another regulatory force—the law—must fill the gap.

3. Thought Experiment: What If Microsoft Started Monitoring?

This Article is not arguing that ISPs must be regulated only because they have the potential to access a vast amount of sensitive information. Falling constraints are the critical part of this argument. A few companies have access to as much or more information about users than ISPs, yet they need not be regulated today. Consider Microsoft. As the developer of Operating Systems (OS) used by more than 90 percent of worldwide users,[184] Microsoft is in a position to know even more about its users than ISPs. It could alter its OS and applications software to give itself access to every network communication sent or received by every Windows-based computer. Microsoft could do even more, monitoring every file saved or modified, every keystroke pressed and mouse movement. It could even install spyware to take snapshots of user screens every few seconds. Unlike an ISP, Microsoft could easily circumvent encryption and track communications regardless of network provider. Even for computers that are only sporadically online, Microsoft could monitor at all times, sending data back whenever it detected a connection to the Internet.

Of course, Microsoft does none of this even though there are no technological constraints in its way, and unlike what is happening to broadband, technological constraints have not fallen in recent times. Furthermore, Microsoft has made no public pronouncements and has re-

180. Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1607–09 (2007).

181. *Id.*

182. *Id.* at 1619.

183. *See supra* Part I.B.

184. Onestat.com, Microsoft's Windows Vista Global Usage Share Is 13.24 Percent on the Web According to OneStat.com, Apr. 1, 2008, http://www.onestat.com/html/aboutus_pressbox58-microsoft-windows-vista-global-usage-share.html ("Microsoft's Windows dominates the operating system market with a global usage share of 95.94 percent.").

vealed no plans indicating the company's moves to monetize user information.[185] Evidently something—probably industry norms and the fear of regulation—has disciplined the company, and we have no reason to believe those forces will not continue to hold sway. For all of these reasons, regulators need not regulate the potential threat of OS monitoring by Microsoft today.

If tomorrow Microsoft began monitoring invasively—imagine it began showing ads targeted to what users were entering into Microsoft Word documents—I would urge regulators to regulate for the same reasons I urge them to regulate ISPs today. It would be evidence that norms or market pressures had shifted, and it would place Microsoft in the same camp as NebuAd, Phorm, AT&T, and Comcast.

In conclusion, given the massive amount of information accessible by ISPs, and in light of the evidence suggesting that ISPs can monitor more invasively than before, we should regulate the worst forms of ISP surveillance. This leaves the question, what can and should we regulate, and how much regulation is enough? As is so often the case with privacy, it comes down to balance.

III. REGULATING NETWORK MONITORING

Part II established that we must skeptically scrutinize ISP claims justifying their new types of invasive monitoring. There are three different claims they tend to make. First, ISPs argue that they respect privacy whenever they anonymize or aggregate the data they collect enough to prevent associations between the data and the user.[186] I conclude in Section B that this is a plausible claim in theory but ultimately often irrelevant in practice.

Second, ISPs claim necessity. They say they cannot provide the services they are hired to provide unless they are allowed to do many kinds of monitoring.[187] In order to assess these claims and provide a specific prescription, Section C takes a detailed, technical look at what ISPs do. Finally, ISPs claim they monitor with their users' consent.[188] Consent is a problematic topic, and I propose a novel mode of analysis in Section D. Before examining these claims in greater depth, let us first dispense with an oft-used but unhelpful metaphor.

185. This reticence is in contrast to the company's open plans to engage in behavioral marketing of those who use its search engine. Saul Hansell, *Ballmer's Catch-22 Problem with Search Ads*, N.Y. TIMES BITS BLOG, July 25, 2008, http://bits.blogs.nytimes.com/2008/07/25/ballmers-catch-22-problem-with-search-ads/ (reporting that Microsoft "was working diligently on narrowing the [search query] advertising gap [with Google]").

186. See *infra* Part III.B for further discussion.

187. *See infra* Part III.C.

188. *See infra* Part III.D.

A. Abandoning the Envelope Analogy

If we adopted the approaches of the past, we would regulate ISP monitoring using the envelope analogy. Telephone privacy is regulated in this manner—we vigorously protect the secrets "within," and barely regulate the information revealed on the outside. Federal law, for example, protects the "content" of communications—defined as "the substance, purport, or meaning of [the] communication"[189]—more vigorously than it protects the non-content "dialing, routing, addressing, or signaling information."[190] We could unthinkingly apply the envelope analogy to the Internet, declaring that a packet is like a closed letter in the mail, with non-content headers stamped outside the envelope and the content sealed within.

Many have done just this. For example, David P. Reed testified to a House Subcommittee that he avoids "defining a whole collection of technical terms by suggesting that you view these Internet Datagrams as *envelopes* containing messages from one host to another on the Internet."[191] Gigi Sohn of Public Knowledge similarly argued that "[Deep Packet Inspection] is the Internet equivalent of the Postal Service reading your mail. . . . ISPs are opening these envelopes, reading their contents, and keeping varying amounts of information about the communications inside for their own purposes."[192] Even those who disagree with these sentiments, such as a DPI industry-supported website, uses the analogy.[193]

Despite its broad adoption, there are many good reasons to avoid this analogy. The envelope analogy states a conclusion rather than provide a tool for coming to that conclusion. But those who use it tend to treat it as an analytic tool, which it is not. Saying that there is an "inside" and an "outside" to a packet is the same thing as saying that we need to draw a line between permissible and impermissible scrutiny, but it offers no guidance about how or where to draw that line. In the quotes above, every speaker assumes away all of the hardest questions by imagining packets as envelopes. Which parts should be deemed inside, and which are outside the envelope?

189. 18 U.S.C. § 2510(8) (2006).

190. 18 U.S.C. § 3127(3). These laws apply to network monitoring as well. See *infra* Part IV.A for more on these laws.

191. *What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Law and Policies: Hearing Before the Subcomm. on Telecomms. and the Internet of the H. Comm on Energy and Commerce*, 110th Cong (2008) [hereinafter *Broadband Provider Hearing*] (statement of David P. Reed, Adjunct Professor, Massachusetts Institute of Technology), http://archives.energycommerce.house.gov/cmte_mtgs/110-ti-hrg.071708.DeepPacket.shtml.

192. *Broadband Providers and Consumer Privacy: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 110th Cong. 15 (2008) (testimony of Gigi B. Sohn, President, Public Knowledge).

193. dpacket.org, Introduction to Deep Packet Inspection/Processing, https://www.dpacket.org/introduction-deep-packet-inspection-processing (last visited Aug. 31, 2009) ("A packet is analogous to a physical postal mail message. The address on the outside of the envelope is analogous to the 'packet header' and the information inside the envelope is analogous to the 'payload.'").

The promise of the envelope analogy is that it is clear and easy to apply, but the solutions proposed to implement the analogy are rarely so clear. For one thing, in the Internet and packet context, there is more than one envelope. Think of a packet like a Russian nesting doll. Packets are built up in successive layers of information with each one wrapped around all of the "inner" layers that have come before through a process called encapsulation.[194] The innermost layer is usually what we consider the "content" of the message—such as the body of the e-mail message or the digital photograph being downloaded from the Web. Outer layers contain many things we consider non-content—such as the addresses used to deliver a message—but they may contain content as well. In large part because of the layered quality of packets, the envelope analogy is at the same time overprotective and underprotective, and it gives rise to question-begging and difficult line-drawing.[195] For these reasons, policymakers should search for an alternative organizing principle.

First, the header-content line is overprotective of privacy because often the content of Internet communications are banal and not likely to cause many privacy harms.[196] The signature my e-mail program appends at the bottom of e-mail messages is not, by itself, terribly sensitive, although it is clearly part of the "content" of each message. That said, a signature could *conceivably* be very important and private. For example, if only one of my computers is configured to attach a particular signature, then the signature becomes a clue to my physical location at the time the message was sent. In other words, the importance of content depends on the context.

Second, the header-content line is underprotective because often the non-content part of the packet is the part that can harm an individual, especially when it is aggregated and correlated with other non-content data across time.[197] The knowledge that a particular user accesses a blog at particular times that correlate to the postings of a notorious anonymous blogger may expose a closely held secret.

Even though the envelope analogy fits poorly with our perceptions of communications privacy, some might want to preserve it because it is supposedly easy to apply. Not so. Because of the layering of network protocols, the line between the inside and outside of the virtual envelope is difficult if not impossible to draw.[198] At any given layer in the Russian-

194. DAVID G. MESSERSCHMITT, UNDERSTANDING NETWORKED APPLICATIONS: A FIRST COURSE 519–20 (1999).

195. *See* SOLOVE, *supra* note 160, at 13 (criticizing earlier conceptions of privacy as being too narrow, too broad, or sometimes both).

196. Solove, *supra* note 143, at 1288 ("Envelope information can be quite sensitive; content information can be quite innocuous.").

197. SOLOVE, *supra* note 160, at 117–21 (discussing the harms that can result from data aggregation).

198. Orin Kerr generalizes the recurring problem with drawing analogies between physical spaces and online constructs. Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357,

doll-like nested layers, all of the interior, encapsulated layers can be called "content."

Take an e-mail message. When composed or read, the line between headers and content seems so solid, it is even drawn as a visible line on the user's screen separating the body of the e-mail message and the header information at the top of the window. Then again, even this clear line is kind of muddy: is the Subject line, which is usually grouped above the line with the headers, content or non-content?

As an e-mail message is being sent across the Internet, the muddy line is muddied further. For example, one could argue that from the ISP's vantage point, only the headers in the outermost IP layer are non-content and that everything encapsulated within is content.[199] If this view were adopted, then ISPs would have no business accessing the To: and From: lines of email messages.

B. Anonymization and Aggregation Are Usually Not Enough

Anonymization and aggregation are techniques for protecting the privacy of people associated with data by omitting important details. Aggregation is the grouping together of information to disclose facts in gross while hiding the details of individuals.[200] Anonymization, in contrast, presents the data at the individual level, but uses techniques—most often a form of encryption called a one-way hash—to obscure the most important details.[201] There can be no denying that we recognize anonymization and aggregation as norms of acceptable disclosure in some contexts. On election night, we do not care—in fact, many of us quite like—when CNN presents vote tallies and pie-chart summaries of surveys about voter sentiment. Even when we are one of the voters surveyed, we would know it is impossible for our personal viewpoints to ever be revealed as a result of these information disclosures thanks to the gross aggregation in the final report and the care with which our identity has been handled in the collection of the information. Even if we cannot produce the mathematical equations, we have a sense that the odds of our "reidentification" from this data are slim.

357–58 (2003). He gives the specific example of comparing the privacy of online communications to physical mail. *Id.* at 365–68.

199. In fact, there are layers "above" IP: the data link and physical layers. From their vantage point, IP information may seem like content. Posting of eck to The Volokh Conspiracy, http://volokh.com/posts/1213821576.shtml#388008 (June 18, 2008, 20:43 EST) ("[A]ll of the TCP/IP info—in your example, TCP port 80 at a given IP address—is 'content' from the perspective of the data link layer (Ethernet, token ring, etc.). I suspect most informed commentators would still say that source/destination IP addresses are addressing info, layer encapsulation notwithstanding.").

200. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. (forthcoming 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

201. *Id.*

Even online, there seems to be a sense that aggregation can protect privacy when the categories are broad and the handling of the data is done with care. At the end of every year, Google summarizes trends in search in a report it calls the Google Zeitgeist.[202] From the 2007 Zeitgeist report, we know that for most of the year, people searched for "Britney Spears" more often than "Paris Hilton," except around the time of Ms. Hilton's arrest and imprisonment.[203] These reports (if not this specific example) offer fascinating windows into the collective mind using the Internet. The reports probably remind readers once each year about the giant iceberg of knowledge Google must possess in order to create this little tip of information. But most probably fret little about the tip itself, because they understand, intuitively if not mathematically, that there is no possibility their searches can ever be revealed through the study of only these graphs and tables.

Given these well-recognized norms, some types of anonymization and aggregation should act as exceptions to prohibitions on the collection, use, and disclosure of information. But ISPs and vendors like Phorm and NebuAd err by treating the word "anonymization" like a talisman for avoiding privacy scrutiny.

1. No Perfect Anonymization

ISPs seem to think that data exists only in a binary state: personally identifiable or perfectly anonymized. We are learning that on the contrary there may be no such thing as perfect anonymization. Worse, we are beginning to suspect that experts tend to underestimate how easy it is to reidentify people from supposedly anonymized data.

Consider the America Online (AOL) data release. In 2006, AOL researchers released twenty million keyword searches submitted by hundreds of thousands of subscribers over a three-month period.[204] Researchers had anonymized the data—or so they claimed—by replacing information which could tie queries to an individual like AOL login IDs with unique identifiers. Although identities could not be revealed directly, all of an individual's searches could be connected to one another through a shared identifier.

What the world learned is that knowing an unidentified person's search queries is often enough to breach privacy. Some of AOL's users, for example, had entered credit card and social security numbers.[205] Others had searched for child pornography or advice on how to kill a

202. Google, Zeitgeist: Search Patterns, Trends, and Surprises, http://www.google.com/press/zeitgeist.html (last visited Aug. 31, 2009).

203. Google, Google Zeitgeist 2007, Showbiz, http://www.google.com/intl/en/press/zeitgeist2007/showbiz.html (last visited Aug. 31, 2009).

204. Nakashima, *supra* note 177.

205. *Id.*

spouse.[206] One wonders whether the FBI submitted subpoenas to learn their identities. Other people provided enough clues in their search strings to allow them to be reidentified, including famous user number 4,417,749, tracked down by the *New York Times*.[207]

AOL appears to have made an honest mistake, but others missed the lesson and are repeating these mistakes. Consider again Phorm and NebuAd, the two services that track the websites visited by users in order to display more targeted advertising. Both companies brag that they anonymize information to protect privacy.[208] I will focus on Phorm because its mechanisms are better documented.[209] Phorm is correct that the steps it takes reduce the risk of reidentification or other harm, but it is laughably wrong when it claims that "all data is anonymous and cannot be attached to any individual."[210]

Just like AOL, Phorm associates web surfing history with a unique identifier.[211] Thus, Phorm knows that user number 1337[212] has visited pages about travel, without having any way to determine the true identity of 1337. Phorm uses another obscuring technique: it does not remember the sites visited, it just remembers the *type* of sites visited.[213] Thus, rather than remember that a user entered "Hawaii Vacation" into Google, Phorm would remember only that the user visited a travel-related web page.

But the ISP who invites Phorm into its network can, if it wanted or was ordered to do so, remember the identity of user 1337.[214] This is not simply information the ISP is already entitled to view, because it is paired with the collection of much more information about user web surfing history than it typically collects today—setting the stage for privacy harm and raising significant questions about provider need and ISP liability. Perhaps what Phorm really meant was that data "cannot be at-

206. *Id.*

207. Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1 (discovering an AOL user based on searches such as "landscapers in Lilburn, Ga" and several people with the same last name of the user).

208. CLAYTON, *supra* note 76; *see also Broadband Provider Hearing*, *supra* note 191, at 3 (testimony of Bob Dykes, Chief Executive Officer, NebuAd, Inc.), http://archives.energycommerce.house.gov/cmte_mtgs/110-ti-hrg.071708.Dykes-testimony.pdf ("[Industry-leading] privacy protections are built into our technology and designed into our policies from the ground up.").

209. CLAYTON, *supra* note 76.

210. Phorm, Frequently Asked Questions, http://www.phorm.com/about/faq.php (last visited Aug. 31, 2009) (partially answering the question, "What type of security measures do you have so that aggregated data is not stolen or lost?").

211. CLAYTON, *supra* note 76, para. 58, at 7.

212. Phorm identifiers are a sixteen-byte value encoded for humans as a twenty-two character string. *Id.* para. 31, at 5. This Article uses shorter numbers for readability.

213. *Id.*

214. *Id.* para. 79, at 9 (noting that user IDs can be linked to IP addresses at the ISP-run "Profiler" and "Anonymizer" machines).

tached to any individual *using only our data*," but it omits the phrase that makes the statement true.[215] This omission is disingenuous, at least.

The complexity of Phorm introduces another set of privacy risks.[216] At some points in the complex flow of data, Phorm's systems have access to the URL being visited by a user, the search queries that led the user to the page, and the ten most frequently used words on the page.[217] Although this data is eventually thrown away,[218] while it is held, it is vulnerable to attack or accidental exposure. This is only one of many points along the chain where much more than the ultimately "anonymized" data can be intercepted.

2. Anonymous Yet Still Invasive

Even if we give Phorm the benefit of the doubt and assume they maintain good security and ignore the threat to privacy from the ISP itself, the Phorm system will still cause privacy harms, despite anonymization. Because the Phorm system ties advertisements to past online behavior, the service itself breaches privacy and causes harm. In an interview about Phorm, security researcher Ross Anderson

> gave the example of a woman who had had an abortion without telling their partner. If she had surfed websites like Mothercare or other baby-related retailers and advice centres while making up her mind about the termination, her family's computers might suddenly start receiving baby ads, creating suspicion from the husband or boyfriend.[219]

Phorm has responded to such concerns by promising to ignore certain classes of information. According to an independent researcher who was briefed on Phorm, the company refuses to keep data (or sell ads) for "adult material, for anything medical, or for alcohol, tobacco, gambling, or politics."[220] This does not entirely address the risk of harm for two reasons.

First, many of these excluded categories seem to be lucrative advertising opportunities, and Phorm will no doubt be tempted to try to recapture some of this lost revenue—particularly if they hit dire financial straits—by shrinking this list over time. Phorm explicitly reserves the right to change the list, saying on its website that "[t]he exclusion list may be added to, or subtracted from, depending on the region of the Internet

215. *See supra* note 210 and accompanying text.

216. CLAYTON, *supra* note 76, para. 79, at 9 (listing eighty steps required to serve monitor user behavior and to serve ads).

217. *Id.* at para. 56, at 7 (describing data held by "Channel Server," a computer in Phorm's control).

218. *Id.* para. 58, at 7.

219. Jim Armitage, *Web Users Angry at ISPs' Spyware Tie-Up*, EVENING STANDARD, June 3, 2008, http://www.thisislondon.co.uk/standard-home/article-23449601-details/Web+users+angry+at+ISPs'+software+tie+up/article.do.

220. CLAYTON, *supra* note 76, para. 80, at 9.

Service Provider."[221] Also, while their official FAQ recites a similar list to that reported by the researcher, instead of "gambling," the FAQ promises to exclude only "Gambling (except National Lottery)," and rather than "politics," the FAQ promises to exclude "UK Political Parties."[222] Perhaps the researcher mistranscribed his list,[223] but even if the FAQ list does not represent a shift in policy, it still reveals the great temptation Phorm feels to define the forbidden categories narrowly. Although a gambling addict may worry about having his lottery habit broadcast to family members, Phorm has evidently decided that this lucrative category was too good to pass up.

The second shortcoming of Phorm's exclusions approach is that it addresses only mainstream embarrassments and secrets, while it utterly fails to protect idiosyncratic privacy. Users who like porn or need medical advice may be protected by Phorm's system, but a user who is embarrassed by something that Phorm's "in-house editorial panel"[224] cannot predict would be embarrassing will be unprotected. People with obscure fetishes or rare addictions may be outed by the Phorm system; professionals who do not want co-workers to know about their love of celebrity gossip are unprotected; those who promise spouses to stop coveting expensive electronics will be revealed. Probably, most people can identify at least one idiosyncratic topic which interests them and would cause at least mild embarrassment if others knew. Phorm's exclusions-based system cannot help them.

Finally, anonymization cannot effectively address the harm to the sense of repose. This harm comes from the fear that one is being watched. It can result in self-censorship. It is not the kind of harm easily offset by hypertechnical arguments about encryption and one-way hash functions. Particularly when the anonymizing party refuses to be completely transparent about its anonymizing methods, the sense of repose can be damaged.[225]

221. Phorm, *supra* note 210 (responding to the question, "What advertising categories are off-limits?").

222. *Id.*

223. On the contrary, the evidence suggests that Phorm vetted Clayton's report carefully. Phorm commented favorably about some aspects of Clayton's report on its own blog. Radha Burgess, *Critic from FIPR Supports Key Phorm Claim*, PHORM BLOG, Apr. 6, 2008, http://blog.phorm.com/user-privacy/critic-from-fipr-supports-key-phorm-claim/. Furthermore, "Phorm's technical people" sent corrections for a handful of errors that Clayton later corrected in an amended report. Richard Clayton, *Twisty Little Passages, All Alike*, LIGHT BLUE TOUCHPAPER, May 18, 2008, http://www.lightbluetouchpaper.org/2008/05/18/twisty-little-passages-all-alike/.

224. Phorm, *supra* note 210 ("Exclusions are based on Interactive Advertising Bureau (IAB) advertising standards and an in-house editorial panel.").

225. SOLOVE, *supra* note 160, at 109 (arguing that "covert surveillance is problematic" because it can "have a chilling effect on behavior").

3. Conclusion

Anonymization is probably never perfect. Even experts seem to underappreciate the likelihood of reidentification as the decision to release the AOL data and the undeserved bragging of Phorm suggest.[226] Because of these risks, policymakers should rarely take an anonymization or aggregation argument at face value. The provider or vendor raising such an argument must face a heavy burden to prove—backed by expert analysis—that their method reduces the risk of reidentification to some acceptably small possibility; simplistic hand-waving will not do. Sometimes, like in the case of Google's Zeitgeist, the argument will be possible to make, but more often, claims about privacy through anonymization should not stand.

Having moved anonymization and aggregation mostly off of the table, providers are left with only two arguments for new invasive monitoring. First, they can argue need. Monitoring might be required to protect the network, to provide service, or for any other legitimate provider goal. In order to assess need, a theory of "reasonable network management" is developed in Section C. Finally, providers can argue that they have received their users' consent. Consent in this context is problematic in ways that will be discussed in Section D.

C. Reasonable Network Management

Why do providers want or need to scrutinize their customers' communications, how does this impact privacy, and does the benefit justify the cost? In this Section, the Article surveys the engineering literature to explain the why, the what, and the future of ISP monitoring.

1. Network Management Defined

The phrase "network management" gained prominence through successive chairmen of the FCC. First, in 2004, Chairman Michael Powell made an influential speech now known as the "Four Internet Freedoms" or "Four Freedoms" speech.[227] In the speech, which has become something of a rallying cry for net neutrality advocates,[228] Chairman Powell described four freedoms consumers had come to expect from

226. *See supra* notes 210–18 and accompanying text.

227. Michael K. Powell, Chairman of the FCC, Preserving Internet Freedom: Guiding Principles for the Industry, Remarks at the Silicon Flatirons Symposium on "The Digital Broadband Migration: Toward a Regulatory Regime for the Internet Age" (Feb. 8, 2004), *available at* http://www.fcc.gov/commissioners/previous/powell/speeches.html.

228. *See Net Neutrality: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 109th Cong. 54 (2006) (statement of Lawrence Lessig, Professor of Law, Stanford Law School) ("It is my view that Congress should ratify Powell's 'Internet Freedoms,' making them a part of the FCC's basic law.").

their ISPs.[229] In elaborating the first freedom, the freedom to access content, he explained, "I recognize that network operators have a legitimate need to manage their networks and ensure a quality experience, thus reasonable limits sometimes must be placed in service contracts."[230]

Powell's successor, Chairman Kevin Martin, thrust network management even more into the telecommunications policy spotlight through a Commission policy statement[231] declaring that the FCC would "incorporate" four principles, modified versions of the four freedoms, "into its ongoing policymaking activities."[232] As a closing footnote elaborated, "The principles we adopt are subject to reasonable network management."[233] This footnote enshrined the concept of network management into policy, if not yet regulation or law, and has since become a significant topic of debate among telecommunications law and policy experts.[234]

Since then, the FCC has given the concept of reasonable network management an oversized role as the line in the sand beyond which regulators need not defer to business judgment and technological decision making. Thus far, however, the line of reasonable network management is vague and indeterminate. Despite the vagueness, the August 1, 2008 Comcast FCC ruling proves the concept has teeth.[235] The fact that "Comcast was not engaging in reasonable network management," according to the FCC gave grounds for the order to cease throttling BitTorrent.[236]

One reason why "reasonable network management" is so vague is it describes not an engineering principle, but a policy conclusion made by weighing the legitimate technological and business goals of network management with what society deems reasonable in light of many principles, including user privacy. The phrase "network management" is a bit easier to define. Several technical books have been written about network management in recent years.[237] These books all struggle to de-

229. Powell, *supra* note 227. The four freedoms are the freedom to (1) access content, (2) use applications, (3) attach personal devices, and (4) obtain service plan information. *Id.*

230. *Id.* at 5.

231. The Policy Statement was signed by all five FCC Commissioners, but commentators have taken to referring to it as Chairman Martin's version of the four freedoms. *See, e.g.*, David S. Isenberg, *How Martin's FCC Is Different from Powell's*, ISEN.BLOG, Aug. 7, 2005, http://www.isen.com/blog/2005/08/how-martins-fcc-is-different-from.html.

232. FED. COMMC'NS COMM'N, FCC 05-151, POLICY STATEMENT IN THE MATTERS OF APPROPRIATE FRAMEWORK FOR BROADBAND ACCESS TO INTERNET OVER WIRELINE FACILITIES 3 (2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.doc.

233. *Id.* at 3 n.15.

234. *E.g.*, Anne Broache, *FCC Wants to Know: Is Degrading P2P Traffic 'Reasonable'?*, CNET NEWS, Jan. 15, 2008, http://news.cnet.com/8301-10784_3-9850611-7.html; Fred von Lohmann, *EFF to FCC: "Reasonable Network Management" Requires Transparency*, EFF DEEPLINKS BLOG, Feb. 29, 2008, http://www.eff.org/deeplinks/2008/02/eff-fcc-reasonable-network-management-requires-transparency.

235. Press Release, *supra* note 105, at 1–2.

236. *Id.* at 2.

237. *See, e.g.*, BENOIT CLAISE & RALF WOLTER, NETWORK MANAGEMENT: ACCOUNTING AND PERFORMANCE STRATEGIES (2007); ALEXANDER CLEMM, NETWORK MANAGEMENT

fine the precise meaning of the phrase,[238] but they end up defining it in similar ways.[239] This Article adopts one of these definitions: "Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems."[240]

As the definition demonstrates, network management requires much more than monitoring; for example, it involves data analysis, incident response, configuration, and planning, just to name some of the most important tasks. Comcast "managed" its network both by looking at BitTorrent packets and by throttling them.[241] But every network management step either involves, or must be preceded by, a network monitoring event; because this Article's central focus is privacy, the Article focuses on monitoring, and the phrases "network monitoring" and "network management" are used interchangeably.

2. Why Providers Monitor

a. The Necessary, the Merely Convenient, and the Voyeuristic

Sometimes providers monitor not out of necessity but out of convenience. The more data an administrator captures, the more likely he will happen to capture the information that reveals the source of a future problem or hard-to-diagnose trend. Overcollection can make up for poor planning, design, and forethought. Threats which could otherwise be addressed through user education, software update management, additional staff, and network design might be mitigated instead through stepped-up surveillance.

Policymakers should not be afraid to question whether expansive, privacy-invading monitoring is truly necessary or merely convenient. Because of the harm to those wrongfully monitored, convenience and efficiency must sometimes be sacrificed to enhance privacy. Then again, no provider should be accused of laziness merely because it has decided

FUNDAMENTALS (2006); DOUGLAS E. COMER, AUTOMATED NETWORK MANAGEMENT SYSTEMS: CURRENT AND FUTURE CAPABILITIES (2007).

238. CLEMM, *supra* note 237, at 5 ("As is the case with so many words, *network management* has many attached meanings."); COMER, *supra* note 237, at 26 ("Unfortunately, network management covers such a broad range of networks and activities that no short definition can capture the task well.").

239. PATRICK CICCARELLI ET AL., NETWORKING BASICS 386 (2007) ("Network management is the process of operating, monitoring, and controlling a network to ensure that it works as intended and provides value to its users."); COMER, *supra* note 237, at 26 ("Intuitively, network management encompasses tasks associated with planning, deploying, configuring, operating, monitoring, tuning, repairing, and changing computer networks."); MANI SUBRAMANIAN, NETWORK MANAGEMENT: PRINCIPLES AND PRACTICE 40 (2006) ("The goal of network management is to ensure that the users of a network receive the information technology services with the quality of service that they expect.")

240. CLEMM, *supra* note 237, at 8.

241. Brad Stone, *Comcast Altering Its Method of Managing Web Traffic*, N.Y. TIMES, Mar. 28, 2008, at C2.

to monitor. The best providers will invest both in planning and surveillance.

Other types of monitoring seem to cross a line from convenience to voyeurism. Websites cite statistics about which operating systems[242] and web browsers[243] their visitors use. Network software and hardware vendors survey the applications used on their networks.[244] Although this type of information can be vitally important for understanding the nature and evolution of the Internet, too often one gets the sense that it is gathered and cited only to satisfy curious minds.

The voyeurs often defend what I call voyeurism as illuminating research into the nature of the network. Policymakers should be wary of claims that collection is necessary for the long-term protection and improvement of the Internet at least when the immediate goals of the study are not clear. Professor Julie Cohen has commented that "[o]ne view, broadly shared among participants on all sides of the [privacy] debate . . . is that the collection and processing of personal data creates knowledge. In addition, because our society places important values on 'sunlight,' withholding or concealing personal data has moral overtones."[245] Cohen questions this view, noting that information is often not the same thing as knowledge, citing the use of genetic markers of disease for insurability and employability or the "knowledge" about what a person wants to buy based on studying behavior.[246] Insofar as ISPs argue that they should be allowed to conduct deep-packet inspection merely to contribute to our understanding of the world, Cohen's critique is worth repeating.[247]

b. Different Networks with Different Priorities

Computer networks come in many different shapes and sizes and serve many different roles. Different kinds of providers have different network management priorities, justifications, and relationships with their users. Thus, the owner of a corporate network inaccessible from the outside world can justify monitoring that we should not permit from the owner of a popular public website. Likewise, the website owner might be able to justify monitoring that an ISP should not be allowed to

242. w3schools.com, OS Platform Statistics, http://www.w3schools.com/browsers/browsers_os.asp (last visited Aug. 31, 2009) (summarizing visitors by operating system used).

243. Browser News, Browser Stats, http://upsdell.com/BrowserNews/stat.htm (last visited Aug. 31, 2009) (collecting browser studies).

244. *Cf.* Ryan Singel, *Internet Mysteries: How Much File Sharing Traffic Travels the Net?*, WIRED, May 5, 2008, http://blog.wired.com/27bstroke6/2008/05/how-much-file-s.html (citing studies tracking how much of the Internet's traffic is dedicated to peer-to-peer).

245. Cohen, *supra* note 153, at 1402.

246. *Id.* at 1404.

247. But ISPs make a more defensible knowledge argument when they talk about defending their network by acquiring the "big picture." Network security experts often talk about "situational awareness," a concept borrowed from the military, the idea that network operators need to gather and mine more data to better detect anomalies. Cert/Coordination Center, Network Situational Awareness (NetSA), http://www.cert.org/netsa/ (last visited Aug. 31, 2009).

do. In order to divide the world of online providers according to the privacy risks they raise, consider this quick, first person tour of the Internet.

At home, I operate a small network of five or six computers. The center of my home network is a *switch*—a small silver box stuffed with inexpensive electronics—which serves multiple roles as the central connection point for the five computers, the WiFi wireless access point, and the gateway to the Internet.[248]

Similarly, in my office at the law school, I run another small network connected to our campuswide network. Administrators in our campus information technology (IT) department manage this huge network with thousands of computers, printers, copiers, wireless access points, and other devices. They have complex and difficult jobs, and it is a struggle for them merely to know what computers are attached to the network, much less to keep the traffic flowing and to prevent bad things from happening.[249] A large professional staff separated into highly specialized duties—security, networking, applications development, server operations, telephony—keeps a close watch on their computers, monitoring and manipulating remote devices, connections between devices, and the data flowing across them all.

I can contact computers on the Internet from both my home network and campus network because both connect directly to ISPs. My home network connects to my cable company, and the campus network connects to several major telecommunications providers—Level 3, Qwest, and ICG—companies that specialize in carrying traffic for large customers with thousands of users.[250] In order to send my communications to destinations outside their own networks, these ISPs purchase Internet connectivity from larger ISPs. These larger ISPs in turn purchase Internet connectivity from even larger ISPs. The largest providers in this pecking order are often called "Tier 1" or sometimes "backbone" providers.[251]

My communications may be handled by two, three, four, or more ISPs en route from my computer to some destination on the Internet. Each one of these ISPs is positioned to know some of my deepest secrets.

248. SCOTT LOWE, HOME NETWORKING: THE MISSING MANUAL 3–7 (2005) (describing routers designed for home use).

249. For a sense of the complexity of running a complex network, browse the computer networking section full of thick tomes in any large bookstore. *E.g.*, EVI NEMETH ET AL., LINUX ADMINISTRATION HANDBOOK (2d ed. 2006) (1001 pages).

250. Some of the University of Colorado's network topology diagrams are posted online. Univ. of Colorado-Boulder, Network Engineering & Operations, http://www.colorado.edu/its/networking/backbone.html (last visited Aug. 31, 2009). For a diagram of our wide area network including links to the providers mentioned in the text, see Univ. of Colorado-Boulder, WAN Connections, http://www.colorado.edu/its/networking/images/WANConnections.gif (last visited Aug. 31, 2009).

251. *See* PRISCILLA OPPENHEIMER, TOP-DOWN NETWORK DESIGN 179 (2d ed. 2004) (discussing Tier 1 providers). Sometimes, attempts are made to define other tiers, of which there are as many as five. *Id.* at 179–80. Because there are no agreed-upon definitions for these lower tiers, this Article will not use Tier 2 through Tier 5.

Of course, I am not the only one exposed, for the bigger the ISP, and the further along they are up the chain, the more secrets belonging to more users they can access. Tier 1 providers may carry the communications of millions of different people simultaneously.[252]

From this brief tour, we can divide the world's providers along two axes corresponding, roughly, to the norms of privacy. The first axis maps the relationship between a user and an ISP. Some providers are *customer-facing*, known to the user as the company at the other end of the cable, the one to whom they send the monthly check.[253] In contrast, *upstream providers* further along the chain are usually unknown to users.[254] Below, I develop the idea that users expect and deserve more privacy from upstream than from customer-facing providers.

A second axis maps the way users use various networks. Users expect and deserve relatively less privacy from *destination providers*, those chosen by the user for applications and services, such as Google for e-mail and calendaring. In contrast, users expect more privacy from *routing providers* which simply carry communications out toward the rest of the Internet, such as ISPs like Comcast and AT&T.[255] Finally, *hybrid providers*, such as my university's IT department, provide applications (e-mail), services (printers), and routing. Users expect a mixed amount of privacy from these providers, treating them sometimes like a destination and sometimes like a conduit.

c. The Purposes of Network Management

Networks are fragile things. Hardware breaks; software crashes, traffic builds, snarling packets in rush hours of congestion, and human beings wreak havoc accidentally or with malicious intent.[256] An unattended large network could probably not survive a day on today's Internet.[257] Every network must be managed.

252. *Id.* at 179.

253. Ingo Busse & Stefan Covaci, *Customer Facing Components for Network Management Systems*, *in* PROCEEDINGS OF THE FIFTH IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT V 31 (Avrel A. Lazar et al. eds., 1997).

254. Some providers are vertically integrated, providing backbone service while selling end-user routing services as well. James B. Speta, *A Common Carrier Approach to Internet Interconnection*, 54 FED. COMM. L.J. 225, 231 (2002).

255. ISPs often provide applications as well, but users may not choose to use them, using only the routing services.

256. JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET: AND HOW TO STOP IT 43–51 (2008) (cataloging online threats).

257. *See* Tom Espiner, *Microsoft Exec Calls XP Hack 'Frightening*,' CNET NEWS, Nov. 13, 2007, http://news.cnet.com/2100-7349_3-6218238.html (describing orchestrated hack into Windows XP computer that took six minutes); Matt Loney, *Study: Unpatched PCs Compromised in 20 Minutes*, CNET NEWS, Aug. 17, 2004, http://news.cnet.com/2100-7349_3-5313402.html (describing researchers who placed unpatched computers on the network that were compromised in twenty minutes); Honeynet Project, *Know Your Enemy: Statistics*, July 22, 2001, http://old.honeynet.org/papers/stats/ (last visited Aug. 31, 2009) (citing older, similar time-to-exploit statistics).

i. The ISP's Core Purpose: Routing

Routing providers, such as ISPs, at the most basic, essential level, *route* packets. Hybrid providers also route packets. Routing requires the scrutiny of only one of the outermost layers in the Russian-doll-like packet: the Internet Protocol, or IP, layer. The IP layer contains, along with a lot of other important information, a header called the destination IP address. An IP address is a unique address for a connected computer, and every computer on the Internet has one.[258] The point of routing is to get a packet to the computer at the destination IP address.

When a router receives a packet, it examines the destination IP address and from it, calculates the "next hop" in the path to the final destination. At least in the ordinary course of things, the destination IP address is the *only* header it must consult. Routing requires no human scrutiny or intervention, thanks to automatic routing protocols.[259]

ii. Four Justifications for ISP Monitoring

Aside from the destination IP address, where do we draw the line for reasonable ISP inspection? What kinds of packet scrutiny *must* network providers perform in order to render particular types of service? What other kinds of scrutiny would a provider prefer to do if it were not forbidden?

To answer these questions, we must look at what else besides routing a provider does.[260] Traditionally, providers of every type have asserted four justifications for monitoring their networks: the need to detect spam, detect viruses, secure the network, and police bandwidth.[261] A few words about each are merited.

258. Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 656 (2003).

259. The most important routing protocol is the Border Gateway Protocol (BGP). *See generally* INTERNET ENGINEERING TASK FORCE, REQUEST FOR COMMENTS 4271, A BORDER GATEWAY PROTOCOL 4 (BGP-4), (Yakov Rekhter et al. eds., 2006).

260. Recently, many have tried rigorously to define what an IT department does, generating an alphabet soup of "frameworks" in an attempt to bring a business-school style of structure and accountability to the field. Two of the most widely used of such frameworks are the Information Technology Infrastructure Library (ITIL), *see* Welcome to the Official ITIL Website, http://www.itil-officialsite.com/ (last visited Aug. 31, 2009), and the Fault, Configuration, Accounting, Performance, Security (FCAPS) system, *see* DOUGLAS E. COMER, COMPUTER NETWORKS AND INTERNETS: WITH INTERNET APPLICATIONS 536–38 (2008).

Of this pair, FCAPS is easier to summarize. As the acronym suggests, FCAPS establishes five purposes for an IT department, most of which can apply to network management: fault correction (recovering from failures and crashes), configuration and operation (setting up new devices and restoring lost configurations), accounting and billing (charging users who pay based on bandwidth or tier of service), performance assessment and optimization (planning capacity and mitigating congestion), and security. *Id.* at 537–38.

The instant discussion avoids these jargon-laden frameworks and tries to describe network management goals in more plain language.

261. *Cf.* Wu, *supra* note 19, at 166–67 (proposing network neutrality principle with six exceptions including protecting the network, limits on bandwidth usage, spam and virus detection, quality of service, and security).

Spam and virus filtering come in many forms but follow the same basic model: computer programs inspect different parts of packets trying to identify spam or viruses. Some of these methods work by matching known unwanted content, while others approach the problem statistically, blocking traffic that behaves like spam or a virus.[262] Some of these methods look deeply into packets, and others look less deep.

The third commonly heard and most nebulous justification is network security. This extremely broad purpose is asserted to justify a wide range of monitoring. Surveillance is necessary, providers claim, to counteract the unpredictable acts of anonymous human agents—hackers and worm authors—who have guile and technical skill.[263] The problem is that when the trigger is a vague, powerful human threat, there is no limit to the amount of monitoring one can justify. I have written about how this style of argument, which I call the Myth of the Superuser, has a pernicious effect in debates about online conflicts.[264] To combat this effect, I have argued that parties asserting the Myth of the Superuser should be held to a high standard of empirical proof.[265]

Finally, consider bandwidth policing, the steps providers take to decrease network congestion. When traffic exceeds a network's capacity, users experience slow performance or worse, system blackouts. Providers commonly raise this justification to oppose calls for network neutrality.[266] They have claimed that mandatory network neutrality will make it impossible for ISPs to cure congestion.[267] To deal with congestion, providers can block or slow (rate-limit) traffic from the users or computers causing the excessive traffic; add more bandwidth; prioritize packets based on application type, a process known as quality of service; or compress the traffic.[268] Some of these techniques require more invasive monitoring than others.

Notice how the strength of all of these justifications can turn on the type of provider making the claim. For example, the network security justification applies to all providers, because given the spread of threats online, we expect all providers to monitor for the protection of their own computers and network, regardless of whether they are customer-facing or upstream, destination, routing, or hybrid.

262. *See* CICCARELLI ET AL., *supra* note 239, at 464–68.

263. *See* Ohm, *supra* note 118, at 1330.

264. *Id.* at 1327.

265. *Id.* at 1385–93.

266. *See* Wu, *supra* note 19, at 153 (reporting that when providers bar users from providing content or providing content to the public, "a major goal is bandwidth management").

267. Matthew Lasar, *Martin Be Damned, Cable ISPs Want Network Management Freedom*, ARS TECHNICA, July 16, 2008, http://arstechnica.com/news.ars/post/20080716-martin-be-damned-cable-isps-want-network-management-freedom.html (paraphrasing two trade association executives warnings that "[i]t's going to be Very Bad . . . if 'network management' is denied its unobstructed due" and that "E-mail, Web browsing, online commerce, video and music will be degraded").

268. David Davis, *Clear Up Network Congestion*, TECHREPUBLIC, Nov. 3, 2005, http://articles.techrepublic.com.com/5100-10878_11-5930741.html.

In contrast, we do not expect and likely do not want some types of providers to filter on our behalf. For example, many residential users opt not to use the e-mail account provided with their broadband connection, choosing to use a webmail provider like Yahoo Mail instead. For these users, their broadband provider should not be scanning their incoming and outgoing e-mail messages for spam or viruses. It both defies expectations and will not work well.

d. The Rise of Deep-Packet Inspection

Providers routinely argue that "shallow packet" monitoring is insufficient to accomplish some of these goals. Automated monitors tend to restrict their view to network-level details, at the IP layer and the next-deepest layer, called the TCP layer, but they can capture only the fact that communications are sent and received without peering into content.[269] At this level, things like spam and viruses are hard to distinguish from other e-mail messages or web surfing behavior.[270]

In order to detect these threats, providers have begun examining much more information, and particularly content information, using automated, always-on DPI tools. DPI tools can identify viruses, by comparing files crossing a network to a database of known viruses; spam, by analyzing the words used; and intruders, by looking at the commands they send.[271] These tools are like packet sniffers because they peer deeply in packets, but they are always on, monitoring every packet passing by.

3. Reasonable Network Management: Provider Need

How do we assess competing claims of ISP need? Need cannot be understood simply by polling affected parties, because ISPs have an incentive to argue for an endless list of needs. Security experts support these arguments by pointing out the innumerable risks providers face online. There is a better way, by referencing external, objective sources like engineering principles—not merely statically as a list of norms, but also dynamically by tracing the *evolution* of such principles—which can give us cues about the value and content of the norms embodied. Professors Mark Lemley and Lawrence Lessig have argued that engineering design principles, "from the very beginning . . . have been understood to

269. *Id.*

270. *See* Jana Dunn, *Security Applications for Cisco NetFlow Data*, SANS INST., July 23, 2001, http://www.sans.org/reading_room/whitepapers/commerical/778.php ("NetFlow logs do not contain the content of the packets associated with the flow, and so are not useful for content-based intrusion detection.").

271. NetworkWorld.com, Deep Packet Inspection, http://www.networkworld.com/details/6299.html?def (last visited Aug. 31, 2009).

have a social as well as a technological significance. They have, that is, been meant to implement values as well as enable communication."[272]

Claims that networks cannot be managed without peering deeply into packets are belied by the decade of evolution of protocols and standards which peer only to shallow depths yet have been widely adopted throughout the industry. If engineers have lived with little more than what these standards have provided for a decade—at least for automated, always-on monitoring as opposed to incident response monitoring—we should weigh recent claims of need to capture more with great suspicion. In order to appreciate the value of looking to engineering standards and protocols, consider instead what would happen if we asked a committee to define the parameters for reasonable network management.

a. A Hypothetical Negotiation

Imagine that policymakers decided to hammer out a new law restricting the type of information an ISP is allowed to collect. One approach would be through negotiation. Policymakers could gather together stakeholders, including all of the ISPs, companies like Phorm and NebuAd, destination providers like Google, the growing DPI industry, and representatives of the user and privacy advocacy communities, to decide what parts of a packet should be presumptively off-limits or fair game to ISP scrutiny.

This would be a frustrating exercise. Providers would tell well-documented tales about the many problems they have experienced that require full-content monitoring. About any proposal declaring part of a packet off-limits, providers would concoct hypotheticals describing how that information might be needed to deal with some subtle nuance of network management. Providers would urge, as an alternative, a flexible and toothless standard based on reasonableness. The exercise would likely end in nothing useful.

Instead of engaging in this frustrating exercise, notice how a natural experiment has taken place over the past decade: Cisco's NetFlow protocol has been released and refined.

b. NetFlow

Cisco has long dominated the router market and, for many network engineers, Cisco's methods and products define the field.[273] In 1996, Cis-

272. Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 930 (2001).

273. John Leyden, *Cisco Dominates Declining Router Market*, THE REGISTER, Sept. 2, 2004, http://www.theregister.co.uk/2004/09/02/router_market_infonetics/.

co created a protocol for network monitoring called NetFlow,[274] building it into its routers ever since.[275] According to a product overview, "NetFlow . . . creat[es] an environment where administrators have the tools to understand who, what, when, where, and how network traffic is flowing."[276]

A Cisco router with NetFlow enabled will monitor every packet, collecting information useful for various purposes, sending it to another computer called a NetFlow collector.[277] NetFlow discards most of the details of every packet, keeping only "a set of 5 and up to 7" attributes.[278] The seven attributes are: (1) IP source address;[279] (2) IP destination address;[280] (3) Source port;[281] (4) Destination port;[282] (5) Layer 3 protocol type;[283] (6) Class of Service;[284] and (7) Router or switch interface.[285] Two other pieces of information are also collected: (8) the amount of data transmitted, in bytes and number of packets; and (9) the date and time associated with each flow.[286] For most network communications, these nine pieces of information are the only pieces of information collected by an ISP.

Using only these nine pieces of information, what can a network operator learn about personal behavior? Imagine a user named Eleanor, a Comcast cable modem subscriber. Every evening after dinner, she logs

274. CISCO SYS. INC., INTRODUCTION TO CISCO IOS NETFLOW 1 (2007), http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.pdf [hereinafter NETFLOW INTRODUCTION].

275. *See id.* at 6.

276. *Id.* at 1.

277. *Id.* at 4.

278. *Id.* at 3.

279. *Id.*

280. *Id.*

281. Ports refer to TCP and UDP ports. Ports can reveal, to some level of confidence, the application (Web, e-mail, instant message, etc.) that generated the packet. Ports will be discussed again in Part V.B.

282. NETFLOW INTRODUCTION, *supra* note 274, at 3.

283. "Level 3" refers to the network layer in both the OSI Reference Model and the Internet Reference Model layers. DOUGLAS E. COMER, INTERNETWORKING WITH TCP/IP: PRINCIPLES, PROTOCOLS, AND ARCHITECTURE 155–71 (5th ed. 2006). Level 3 protocol type will distinguish, for example, between IPv4 and ICMP data.

284. Class of Service (CoS) is associated with Quality of Service (QoS), a buzzword in the net neutrality debates. Briefly, a network packet or frame flagged with a CoS field can be categorized as of a higher or lower priority than other communications. *See generally* GILBERT HELD, QUALITY OF SERVICE IN A CISCO NETWORKING ENVIRONMENT (2002). Video, for example, might be flagged with a high CoS so that a QoS system can shuttle it to the front of the line. *Id.* at 28 (listing seven user priority levels from 1 (background) to 7 (network control/critical) with 6 meaning "interactive voice").

285. A router's interfaces are the ports into and out of the router. A router connected to four networks, for example, would have four interfaces.

286. NETFLOW INTRODUCTION, *supra* note 274. Actually, a few other pieces of information—not important for this discussion—can also be stored with an IP Flow. For example, IP Flows can contain NetFlow version number, flow sequence number (1 for the first flow, 2 for the second, etc.), aggregated TCP flags, and routing information. CISCO SYS. INC., CISCO IOS SWITCHING SERVICES CONFIGURATION GUIDE PART 3: NETFLOW OVERVIEW (2001), http://www.cisco.com/en/US/docs/ios/12_1/switch/configuration/guide/xcdnfov.pdf; CISCO SYS. INC., NETFLOW SERVICES SOLUTIONS GUIDE (2007), http://www.cisco.com/en/us/docs/ios/solutions_docs/netflow/nfwhite.html.

on. In a typical session, she accesses her email account several times, reading twenty messages and sending five. She also surfs the web, visiting thirty different websites and using Google's search five times.

Using NetFlow data alone, Comcast can learn that Eleanor sent five e-mail messages[287] and read twenty.[288] For each website Eleanor visited, Comcast can note the IP address of the computer hosting the website, track the time and date of each visit, and determine how much data Eleanor downloaded. What Comcast knows is dwarfed by what it cannot know because NetFlow forgets so much. Comcast cannot know the e-mail addresses of the other parties on the twenty-five e-mail messages.[289] Nor can Comcast obtain copies of the "Subject" lines, message bodies, or file attachments for any of those e-mail messages.

Although Comcast knows the IP addresses of the websites Eleanor has visited, it cannot know much else about her surfing habits. For one thing, because smaller websites often share IP addresses with other websites,[290] Comcast will often not be able to infer the precise sites Eleanor has visited, even though it might be able to narrow down a list of possibilities. Even more importantly, NetFlow data does not preserve any of the information packed into the Uniform Resource Locators (URLs) Eleanor has visited. A URL is the long string of characters that appear in the web browser's address bar, such as http://www.google.com/search?q=network+management. This is critical because often the URL can reveal a lot of personal information. For example, Comcast will not have access to Eleanor's Google search queries, *New York Times* reading patterns, or Amazon.com book browsing history, all of which are decipherable to someone with access to URLs.

287. E-mail is usually sent using the Simple Mail Transfer Protocol (SMTP) protocol, which is usually sent to port 25. *See generally* INTERNET ENGINEERING TASK FORCE, REQUEST FOR COMMENTS 2821: SIMPLE MAIL TRANSFER PROTOCOL (J. Klensin ed., 2001) (defining ESMTP, the successor to SMTP). Because IP Flows preserve port numbers, the number (and date and time) of Eleanor's outgoing e-mail messages will be kept.

288. If Eleanor uses the older Post Office Protocol Version 3 (POP3) for reading e-mail, the provider might only be able to tell that Eleanor downloaded messages to her computer but might not be able to see how many Eleanor downloaded and read. *See* INTERNET ENGINEERING TASK FORCE, REQUEST FOR COMMENTS 1939: POST OFFICE PROTOCOL—VERSION 3 (J. Myers & M. Rose eds., 1996). On the other hand, if Eleanor used Internet Message Access Protocol (IMAP) for reading mail, Comcast might also be able to tell how many messages Eleanor actually read. *See* INTERNET ENGINEERING TASK FORCE, REQUEST FOR COMMENTS 3501: INTERNET MESSAGE ACCESS PROTOCOL—VERSION 4REV1 (M. Crispin ed., 2003).

289. Comcast does not know this from NetFlow data alone, but they may also run Eleanor's outgoing mail server using the SMTP protocol. *See supra* note 287. Most SMTP servers log the "To:" information for outbound e-mail and the "From:" information for inbound e-mail. O'Reilly Media, *Getting Started with Sendmail*, DEVELOPER SHED, July 7, 2005, § 1.10, http://www.devshed.com/c/a/Administration/Getting-Started-with-Sendmail/12/ (describing sendmail's logging function with default logging of "successful deliveries"); Anton Chuvakin, *Anton Security Tip of the Week #5: Sendmail Log Adventures*, O'REILLY SYS ADMIN, Nov. 6, 2006, http://www.oreillynet.com/sysadmin/blog/2006/11/ (showing sample log entry for successful mail delivery under sendmail).

290. This is through a mechanism known as virtual hosting. BEN LAURIE & PETER LAURIE, APACHE: THE DEFINITIVE GUIDE 86–93 (3d ed. 2003) (describing virtual hosting).

NetFlow data will contain no trace of cookies or bookmarks. NetFlow will not track the type and version of Eleanor's browser software nor the type and version of computer Operating System, even though Eleanor's browser reveals this information to every website she visits. Data entered into web-based forms will not be stored. If Eleanor prints or saves web content, the fact that she has done this is not transmitted on the network at all. Comcast cannot track how long she keeps her browser open to a particular page or what parts of a given page she reads.

In sum, NetFlow, which is the single most important tool used by network engineers today,[291] provides a privacy balance. It gives network engineers a broad window into the activity on their networks, but it throws away much of the most sensitive data.

c. NetFlow as a Ceiling on Automated Monitoring

Notice how the development of the NetFlow protocol tackles the same problem as the hypothetical public negotiation described earlier. NetFlow has always been about tradeoffs: given technological constraints preventing complete monitoring, what are the essential pieces of information needed to manage a network? If many providers over the years had needed to save the entire URL in addition to the IP address in order to manage a network, they could have lobbied Cisco to make this change. The fact that Cisco never made this change suggests that the URL, no matter how useful it might be for some provider purposes, was not widely useful for network management.

The evolution of NetFlow is, in fact, better than the hypothetical negotiation precisely because it occurred outside the public spotlight. The purity of the task set before Cisco—help customers manage their networks given technological constraints—and the absence of legislators and lawyers during the process should give us great confidence that this list is an untainted distillation of engineering need.

For these reasons, policymakers should look to the NetFlow list as a first-order cut at the type of monitoring necessary for network management. Putting it more directly, policymakers should declare the NetFlow list to be a ceiling[292] on the classes of data an ISP may capture automatically, at least without a specific justification. Or, to restate it more palatably for providers, routing providers who gather nothing but data listed in the NetFlow list should be presumptively within their rights. The NetFlow list thus serves as a rejoinder to latter-day, opportunistic claims of need for invasive monitoring. You don't need more than the NetFlow

291. *See* Cristian Estan et al., *Building a Better NetFlow*, 34 COMPUTER COMM. REV. 245, Aug. 2004, at 245, 246 ("NetFlow . . . is the most widely used flow measurement solution today."). *But see infra* note 294 (discussing surveys finding surprisingly low usage of NetFlow).

292. Of course, the NetFlow list might be too privacy invasive, which is why it is a ceiling and not a floor. Policymakers might determine that one or more of the fields in the NetFlow list reveal too much private information.

list, the argument goes, because you have been able to run your networks with little more than this for a decade or more.

Several objections to this proposal are anticipated. First, providers will emphasize that NetFlow is but one tool of many used in network management. Most providers supplement NetFlow with a host of other logging capabilities that capture other kinds of data.[293] Some providers do not use NetFlow at all.[294] Despite these true claims, no other form of automated monitoring enjoys the widespread adoption or long history of use that NetFlow has.[295]

Second, providers might complain that NetFlow represents the idiosyncratic choices of one vendor, Cisco, and should not bind an entire industry. On the contrary, the Internet Engineering Task Force (IETF)—the organization of network researchers that sets standards for the Internet—has recently begun to develop a protocol for automated network monitoring called IPFIX.[296] After canvassing many alternatives, it selected NetFlow as the model for IPFIX.[297] This is an external validation from a much broader coalition of scientists and vendors about the appropriateness of the design.

d. Routine Monitoring Versus Incident Response

NetFlow should be used as a measuring stick for automated monitoring only. Monitoring needs change considerably when a hacker is thought to have breached network security or a worm, virus, or denial of service attack is suspected. Any regulation of network monitoring must allow more provider leeway during incident response.

For example, can an investigator track a hacker using NetFlow data alone? It is extremely unlikely, because the hacker will usually use ordinary protocols to transmit scans and attacks. Policymakers should allow DPI during the hot pursuit of an intruder or active tracking of a worm or virus.

If a monitoring exception is carved out for incident response, several limits should be enacted to prevent the exception from swallowing the

293. *See* Drew Robb, *Going with the Netflow for Network Management*, ENTERPRISE NETWORKING PLANET, Jan. 20, 2009, http://www.enterprisenetworkingplanet.com/netsysm/article.php/3797511.

294. Brad Reese, *NetFlow Is Not Being Used by 77 Percent of IT Professionals*, NETWORK WORLD'S CISCO SUBNET BLOG, June 23, 2008, http://www.networkworld.com/community/node/29224 (reporting results of survey of 600 IT professionals, noting that only 23 percent of respondents used NetFlow but noting that respondents from larger providers had a higher usage rate). *But see* Estan et al., *supra* note 291, at 246 ("NetFlow . . . is the most widely used flow measurement solution today.").

295. We must be careful not to confuse the kind of automated logging done by application providers as opposed to routing providers. E-mail providers typically log a bit of information about every e-mail message sent or received. Website owners typically log every visit to the site.

296. *See* INTERNET ENGINEERING TASK FORCE, IP FLOW INFORMATION EXPORT (IPFIX) CHARTER, http://www.ietf.org/html.charters/ipfix-charter.html (last visited Aug. 31, 2009).

297. S. Leinen, *RFC 3955: Evaluation of Candidate Protocols for IP Flow Information Export (IPFIX)*, THE RFC ARCHIVE, Oct. 2004, http://www.rfc-archive.org/getrfc.php?rfc=3955.

rule. First, incident response must be for a limited time. Second, the investigator should be obligated to narrow her scope by filtering out known innocuous traffic whenever possible. Third, although collection restrictions should be liberalized, providers should be forbidden from using the products of incident response for purposes unrelated to the investigation. They should not, for example, be allowed to use the data collected for marketing.

D. Rethinking Consent

Providers argue that users should be entitled to consent to monitoring in exchange for something of value, such as the service itself or something additional like targeted advertising.[298]

1. Conditions for Consent

Much has been written about information privacy and consent. In fact, it is not much of an exaggeration to say that *most* of what has been written about information privacy has been about consent. The scholars who identify as the members of the New Privacy movement position themselves as a reaction to the information-commodification strain of writers who had come before and who had trumpeted the concept of consent and market alienability of information privacy.[299] A fine representative example comes from Paul Schwartz. In his article *Internet Privacy and the State*, Schwartz incisively critiques the idea of self-determination in cyberspace.[300] He finds instead that information asymmetries, collective action, bounded rationality, and a lack of meaningful alternatives contribute to what he calls an "autonomy trap."[301]

These writers have not abandoned consent completely. Julie Cohen, another writer associated with the movement, urges forcefully for strong data protection legislation, but she concedes that a consent exception would be appropriate in such a law because "people may have legitimate reasons for trading privacy for value in particular cases."[302] Still, in order to offset "data-processing practices [that] provide individuals with . . . little information about the uses of personally-identified data, and their associated costs and benefits," she would ask regulators to define in their law "the conditions for effective consent."[303] In elaborating this idea, she uses the metaphor of distance, arguing that "the farther removed a particular use of personally-identified data is from its initial

298. *See, e.g.*, Joann M. Wakana, Comment, *The Future of Online Privacy: A Proposal for International Legislation*, 26 LOY. L.A. INT'L & COMP. L. REV. 151, 172 (2003).

299. *See* Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1, 22 (explaining the primary arguments of the New Privacy Scholars).

300. Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 821–22 (2000).

301. *Id.* at 821.

302. Cohen, *supra* note 153, at 1432.

303. *Id.* at 1432–33.

collection—whether in terms of subject matter, time, or the nature of the entity making the use," the less willing we should be to recognize consent as valid.[304]

This is an intriguing idea because it looks at the consent question as an architectural question to be resolved categorically instead of an individualized assessment of the facts in a particular case. In some situations, an examination of the structure of consent—how was it solicited? how was it acknowledged?—can be as illuminating (or more illuminating) than a study of the actual terms of consent. This is consistent with information privacy scholars who urge a shift in attention from individual harms to structural and architectural problems. Daniel Solove thinks about privacy "as an aspect of social and legal structure."[305] Neil Richards praises this argument for "shifting the focus of the harms caused by increased information flow from anecdotal instances of information disclosure to the power implications of those increased flows."[306]

What are the architectural features of online consent, and do they give us reason to respect or ignore the types of consent usually used to justify ISP monitoring?

2. The Proximity Principle

The architectural legitimacy of consent can be measured by what I am calling the *proximity principle*. The more closely related—or proximate—a user or customer is to a provider, the more a claim of consent should be upheld as valid.

Two factors weigh in measuring proximity: (1) the level of competition for the service provided, and (2) the nature of the channels of communication between the provider and customer. The first factor asks whether the customer supposedly consenting to be monitored had any meaningful choice about what provider to use. The second factor assesses the mechanisms for asking for and receiving consent, disfavoring the use of buried privacy policies on which ISPs place great stock.

Today, customers have meaningful choice among e-mail providers. A customer can elect to use the account offered by his or her broadband ISP; a webmail provider such as Gmail, MSN Hotmail, or Yahoo!; or another smaller third-party e-mail provider.[307] Almost all e-mail providers offer e-mail for free. Customers also enjoy competition and choice for many other online services such as instant messaging, VoIP, blog hosting, and web hosting.[308] They tend also to have many choices for des-

304. *Id.* at 1432.
305. SOLOVE, *supra* note 145, at 97.
306. Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1097 (2006).
307. Ohm, *supra* note 299, at 44.
308. *See* Recent Development, *Splog! Or How to Stop the Rise of a New Menace on the Internet*, 19 HARV. J.L. & TECH. 467, 469–70 (2006).

tination providers such as search, news, shopping, and increasingly, video delivery.[309]

Because users enjoy so many choices for all of these services and destinations, they are likelier to consent meaningfully when using them. With so many choices, there is an opportunity for competition on privacy terms. Many privacy-sensitive consumers, for example, refuse to use Gmail because Gmail shows contextual advertising keyed to the content of e-mail communications.[310] For these users, there are many similar competitors who do not show contextual advertising.[311] Abundant choice also makes it more likely that a customer has received a genuine benefit as consideration.

In contrast, customers have very little choice about broadband connectivity. In most parts of the United States, the only two choices are DSL from the telephone company and a cable modem from the cable company.[312] Upstream providers such as Tier 1 providers present no customer choice. A user has no say or even knowledge about the commercial contracts between her ISP and upstream ISPs.

Second, proximity turns on the nature, quality, and quantity of the communication channels between the user and the provider. Again, this is a categorical, architectural assessment, not a user-by-user calculation, of the sort a judge might undertake to measure whether a particular plaintiff consented. One way to express this is to borrow the old telephone concept of "in band" and "out of band" communications. When A is talking to B on a telephone, the things they are saying are carried in-band. If a telephone operator had to break into the call to ask a question, it would do so in-band, by joining the conversation. Communications that arrive through some mechanism other than the voice channel are out-of-band.

Some providers communicate in-band every time the user accesses the provider's service. Web-based e-mail, or webmail, providers, for example, require users to login every time they visit the site. This gives the webmail provider ample opportunity to send "in-band" messages to the user. If a major change to a privacy policy is needed, the webmail provider could print prominent text above the login prompt that said "Notice: Our privacy policy has changed. Please click here to read about the

309. *See* Michael Zimmer, *Privacy on Planet Google: Using the Theory of "Contextual Integrity" to Clarify the Privacy Threats of Google's Quest for the Perfect Search Engine*, 3 J. BUS. & TECH. L. 109, 109–10 (2008).

310. *See Google's Gmail Sparks Privacy Row*, BBC NEWS, Apr. 5, 2004, http://news.bbc.co.uk/2/hi/business/3602745.stm.

311. *See* Saul Hansell, *Take That, Google: No Ads from Apple*, N.Y. TIMES, June 9, 2008, http://bits.blogs.nytimes.com/2008/06/09/take-that-google-no-ads-from-apple/.

312. Kim Komando, *Broadband Options Besides DSL and Cable Emerging*, MICROSOFT SMALL BUS. CENTER, at 1-2, http://www.microsoft.com/smallbusiness/resources/technology/broadband-mobility/broadband-options-besides-DSL-and-cable-emerging.aspx#Broadbandoptionsbesides DSLandcableemerging ("In most cases, you have two decent broadband choices: cable and digital subscriber line (DSL).").

changes, and by logging in to your account, you accept the changes." Other providers, like some instant messaging providers, require a single, in-band interaction with the provider during account creation without subsequent communications. This is a less proximate relationship than the service that requires a login every day, but it still presents the opportunity to impart privacy policies at least once, during account creation.

3. ISPs and Proximity

In contrast to the two in-band examples just given, customers rarely communicate in-band with their broadband provider. The majority of users call a DSL or cable modem salesperson on the telephone to establish service. At least in my experience, never does the salesperson read the terms of service over the phone. Sometimes, privacy policies are included with the first bill in the mail often buried among a pile of ads, also out-of-band.

Under both factors, ISPs are not very proximate to users. There is little choice in the broadband market and ISPs typically do not and cannot communicate with users in-band. This conclusion is not irreversible; providers have the power to increase their proximity to users. An ISP could convince a user to begin using its e-mail service or web hosting service, perhaps by competing on price, service, or convenience, which would convert the ISP into a hybrid provider, with opportunities for consensual monitoring. An ISP could also refuse to route any packets to a user unless he first viewed a mandatory "captive portal," like those commonly seen on free wireless and hotel networks, which first require the user to click "I agree." If an ISP refuses to take these proximity-enhancing steps, users should never be allowed to consent to wholesale ISP monitoring.

IV. THE LAW

Some of the principles presented above—exceptions based on provider need, the proximity principle, and a skeptical view of user consent—are already built into one type of law, the wiretapping laws. These laws are imperfect, and an overhaul will be proposed in Section B, but generally they adhere well to the principles. Under these laws, many of the aggressive new forms of ISP monitoring described in Part I sit beneath a legal cloud. Providers will likely be sued and may even be criminally prosecuted if they continue to engage in the aggressive monitoring they have begun to embrace.

A. The Law of Network Monitoring

1. ECPA: Prohibitions

Federal and state wiretap laws are the principal privacy laws regulating packet sniffing and automated network monitoring. The following discussion focuses primarily on federal law, upon which many of the state laws are based. The Federal Wiretap Act was first enacted in 1968 at which time it regulated only telephone wiretaps and hidden microphones.[313] In 1986, Congress enacted the ECPA, amending the law to govern the interception of electronic communications.[314]

a. Few Obvious Answers

As many courts[315] and scholars[316] have complained, the ECPA is confusing. The Fifth Circuit has complained that the Act "is famous (if not infamous) for its lack of clarity,"[317] a statement that the Ninth Circuit rejoined "might have put the matter too mildly."[318] Professor Orin Kerr blames this confusion on the unfortunate combination of "remarkably difficult statutory language"[319] and the dearth of cases construing the statute.[320] The rules are particularly confusing for ISP monitoring, because so many exceptions in the law apply to providers, and because courts have had little occasion to consider ISP monitoring. It is difficult, therefore, to make confident predictions about how courts will rule. Some of the following discussion will be confident and certain, but much of it will be expressed with some doubt.

But the doubt runs both ways: there is neither clear liability nor immunity for many recent provider acts under the law. Given the stakes, responsible companies should err on the side of avoiding new, invasive forms of monitoring that raise the risk of illegal behavior.

b. Wiretap Prohibitions

Packet sniffing falls within the prohibited conduct of the ECPA and most state wiretap laws. The ECPA makes it illegal to "intentionally in-

313. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2511–2520 (2006)).

314. Electronic Communication Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 28 U.S.C.).

315. United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).

316. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 820 (2003) ("The law of electronic surveillance is famously complex, if not entirely impenetrable.").

317. *Steve Jackson Games*, 36 F.3d at 462.

318. *Smith*, 155 F.3d at 1055.

319. Kerr, *supra* note 316, at 821.

320. *Id.* at 823–24.

tercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication."[321] An electronic communication is, in part, "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature."[322] Intercept means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[323]

Putting these three provisions together, courts have held it at least a prima facie Wiretap Act violation to copy e-mail messages before they are delivered;[324] to obtain a cookie from a customer's computer;[325] and to install and use spyware to capture chat conversations, instant messages, e-mail messages, and websites visited.[326] These are all actions that ISPs engaged in aggressive monitoring might undertake.

Any person whose communications are intercepted may bring a federal, civil lawsuit against the wire tapper.[327] Liable defendants must pay actual damages to the victims or statutory damages of $100 per victim per day or $10,000 per victim, whichever is greater.[328] Wiretapping is a federal felony investigated by the FBI with a maximum penalty for first-time offenders of five years in prison.[329]

c. Pen Registers and Trap and Trace Devices Act

The envelope analogy is embedded in the ECPA, but not in the way some people think. Some commentators mistakenly claim that it is *legal* to acquire non-content information.[330] On the contrary, although non-content collection falls outside the Wiretap Act's prohibitions, the ECPA created a separate law prohibiting the collection of non-content information.

The Pen Register and Trap and Trace Act (Pen Register Act)[331] regulates the installation and use of devices that "record[] or decode[]"

321. 18 U.S.C. § 2511(1)(a) (2006).
322. *Id.* § 2510(12).
323. *Id.* § 2510(4).
324. United States v. Councilman, 418 F.3d 67, 85 (1st Cir. 2005) (en banc).
325. *In re* Pharmatrak, Inc., 329 F.3d 9, 22 (1st Cir. 2003).
326. O'Brien v. O'Brien, 899 So. 2d 1133, 1137 (Fla. Dist. Ct. App. 2005) (construing state statute modeled after federal wiretap law); *accord* Potter v. Havlicek, No. 3:06-CV-211, 2007 WL 539534, at *8–9 (S.D. Ohio Feb. 14, 2007) (holding use of keystroke and screen shot logging software to be likely ECPA violation).
327. 18 U.S.C. § 2520(a).
328. *Id.* § 2520(c).
329. *Id.* § 2511.
330. Nancy J. King, *Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices*, 60 FED. COMM. L.J. 229, 289 (2008) ("[O]ne important limitation of the ECPA's privacy protections is that it only protects the contents of electronic communications from unlawful interception or access; it does not broadly protect consumers' information privacy with respect to their personal data.").
331. 18 U.S.C. §§ 3121–3127.

non-content information.[332] Although there might have been some doubt at one point whether this applied to the Internet, section 216 of the USA PATRIOT Act extended this provision to devices that record or decode "dialing, routing, addressing, or signaling information."[333] This is a broad phrase, which undoubtedly encompasses IP addresses, e-mail "To:" and "From:" addresses, and other non-content routing information. The Pen Register Act makes it a crime (a misdemeanor) to install or use devices to record or decode such information, subject to a number of exceptions.[334]

The Pen Register Act is a flawed statute.[335] Most notably, the Pen Register Act has only three statutory exceptions while the Wiretap Act has dozens.[336] For example, it is not a Wiretap Act violation to intercept communications "readily accessible to the general public" but there is no comparable exception in the Pen Register Act.[337] This could lead to the anomalous result of a court finding criminal culpability for the collection of non-content information that would have been justified if content information had been collected instead. Worse, a court might rule a single act both legal, with respect to the content captured, and illegal, with respect to non-content.

ISPs face no civil liability for non-content monitoring,[338] and given the lack of prosecutions under this statute—misdemeanor prosecutions tend not to motivate federal law enforcement agents[339]—they probably do not face criminal prosecution either. This might embolden some ISPs to defy these rules. This is unwise for several reasons. First, if ISPs willfully violate the Act in order to perform some unprecedented, invasive monitoring, law enforcement agents and prosecutors may be motivated to investigate and prosecute. Second, an ISP's lawyer violates her ethical obligations if she advises her client to violate a criminal law.[340]

332. *Id.* § 3121(c).

333. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288–90.

334. 18 U.S.C. §§ 3121–3127.

335. *See generally* Robert Ditzion, Note, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1321 (2004) (arguing that the pen register fits poorly to the Internet).

336. *Compare* 18 U.S.C. § 3121(b) (listing all of the Pen Register Act exceptions), *with* 18 U.S.C. § 2511(2) (listing some of the Wiretap Act exceptions).

337. 18 U.S.C. § 2511(2)(g)(i).

338. Under California's Unfair Competition Law, CAL. BUS. & PROF. CODE § 17200 (West 2008), injured customers of an ISP might be able to sue to recover damages for violations of the Pen Register Act. *See* Diaz v. Allstate Ins. Group, 185 F.R.D. 581, 594 (C.D. Cal. 1998) ("Under California law, a private plaintiff may bring action under unfair competition statute to redress any unlawful business practice, including those that do not otherwise permit a private right of action . . . .").

339. *Cf.* Sameer Bajaj, Note, *Policing the Fourth Amendment: The Constitutionality of Warrantless Investigatory Stops for Past Misdemeanors*, 109 COLUM. L. REV. 309, 334 (2009) ("To extract a bright-line rule from the *Terry*/*Brown* reasonableness test declaring all completed misdemeanor stops unconstitutional, one must posit that misdemeanors are universally qualitatively distinct from felonies such that the governmental interests in preventing or solving them are always comparatively lesser.").

340. *See* MODEL RULES OF PROF'L CONDUCT R. 1.2(d) (2004).

d. Stored Communications Act

The ECPA also created the Stored Communications Act (SCA).[341] The SCA restricts access to some communications in storage.[342] ISPs need not worry about this prohibition, however, because unlike the Wiretap and Pen Register Acts, ISPs receive blanket immunity under the SCA.[343]

This blanket immunity for access to stored communications might warp into a safe harbor from Wiretap Act liability as well, given a series of misguided cases. These cases, most notably the Ninth Circuit's opinion in *Konop v. Hawaiian Airlines, Inc.*,[344] stand for the proposition that a single allegedly wrongful action arises under either the SCA *or* the Wiretap Act, but never under both.[345] The precise reasoning is elaborate, tortured and not worth illuminating fully in this Article.

The most recent United States Court of Appeals opinion about this issue refused to follow the misguided *Konop* rule. In *United States v. Councilman*,[346] the First Circuit en banc concluded that an act could be charged under both the SCA and Wiretap Acts.[347]

Even if other courts opt for the *Konop* rule instead of the *Councilman* rule, ISPs are not necessarily in the clear. First, in order to fall under the *Konop* rule, the monitoring must occur on communications "at rest," even if only for split seconds.[348] When ISPs monitor, they tend to do so on routers or in firewalls, when messages are still "in motion." Thus, a court could follow *Konop* yet rule that ISP monitoring falls on the Wiretap side of the divide. Finally, *Konop* says nothing about liability under the Pen Register Act, and it is unlikely that the reasoning could be extended to that Act.

2. ECPA: Defenses and Immunities

Under the wiretap laws, may AT&T use deep-packet inspection and other network management techniques to monitor for copyrighted materials? Did Comcast break the law by peering into user packets in order to identify and throttle BitTorrent transfers? May Charter, NebuAd,[349]

341. 18 U.S.C. §§ 2701–2122 (2006).

342. *Id.* § 2701(a).

343. *Id.* § 2701(c)(1) ("Subsection (a) of this section does not apply with respect to conduct authorized by the person or entity providing a wire or electronic communications service.").

344. 302 F.3d 868 (9th Cir. 2002).

345. *Id.* at 878–79. Other cases arguably supporting this conclusion include *United States v. Smith*, 155 F.3d 1051, 1057 (9th Cir. 1998), and *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 461–62 (5th Cir. 1994).

346. 418 F.3d 67 (1st Cir. 2005) (en banc). I served on the Department of Justice's team representing the United States in the en banc proceeding of this case.

347. *Id.* at 82.

348. *Konop*, 302 F.3d at 878 n.6.

349. NebuAd's plans have inspired dueling memos debating whether the service violates the Wiretap Act. *Compare* Ctr. for Democracy & Tech., An Overview of the Federal Wiretap Act, Elec-

and Phorm monitor the websites its users visit? At least under federal law, there are three statutory exceptions within which these acts might fall: "rights and property," "rendition of service," and consent.[350] There are arguments for and against the application of these exceptions to these fact patterns, and none of these arguments are irrefutably correct.

a. Protection of Rights and Property

The first two exceptions are provided in the same section of the federal statute:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity *which is a necessary incident to the rendition of his service* or *to the protection of the rights or property of the provider of that service . . . .*[351]

Consider first the permission to protect "rights and property." This exception raises all of the issues of provider need, as discussed in Part III. This exception does not grant ISPs blanket immunity to conduct any type of monitoring for any reason.[352] The exception is structured as a means-justifications test. Regarding justifications, interception is not illegal when done to protect a provider's "rights and property," an undefined and somewhat vague phrase.[353] As for means, an interception is legal only if it is a "necessary incident" to protecting rights and property.[354]

The adjective "necessary" in "necessary incident" dictates a searching and skeptical review of the fit between justifications and methods of

tronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising (July 8, 2008), http://www.cdt.org/privacy/20080708ISPtraffic.pdf [hereinafter CDT Wiretap Analysis], *with Broadband Provider Hearing*, *supra* note 191, at 10–18 (testimony of Bob Dykes, Chief Executive Officer, NebuAd, Inc.), http://archives.energycommerce.house.gov/cmte_mtgs/110-ti-hrg.071708.Dykes-testimony.pdf (appending NebuAd, Inc. memo to his testimony).

350. There are other exceptions, but none that bear a lengthy elaboration. Providers might argue that traffic sent onto the Internet is "readily accessible to the general public," which is legal to acquire under the Wiretap Act. 18 U.S.C. § 2511(2)(g)(i) (2006).

Also, ISPs might invoke the so-called business telephone extension exception. 18 U.S.C. § 2510(5). This exception to the Wiretap Act permits customers and users to use so-called telephone extensions without worrying about wiretapping liability.

One court, however, has interpreted this exception much more broadly. In *Hall v. Earthlink Network, Inc.*, the Second Circuit interpreted this provision to apply to any technology used in the "ordinary course of business." 396 F.3d 500, 504–05 (2d. Cir. 2005). Although a full discussion of *Hall* is outside the scope of this Article, the opinion is flawed in many ways and should not be followed. This exception was always intended as a backwater, a way for telephone companies and stores to check on the quality of their telephone support staff and nothing more. A backwater it should remain.

351. 18 U.S.C. § 2511(2)(a)(i) (emphasis added).

352. Compare the blanket immunity found in the SCA. *Id.* § 2701(c)(1).

353. *See id.* § 2511(2)(a)(i).

354. *See id.*

monitoring. Providers should bear a heavy burden to show that their network management choices are tightly connected to their asserted justifications. Congress could have used the more deferential phrase "reasonable incident," but it chose a much stricter formulation instead.

Some courts have defined this very strictly, saying that the provider must show that the monitoring "could not have been conducted less extensively and that the [provider] could not have employed other reasonable measures" to address the justification.[355] One court required a "substantial nexus" between the monitoring and the reason for the monitoring,[356] a seemingly more deferential standard, but even that court suppressed some records having nothing to do with the purpose of the investigation.[357]

Other courts have rejected provider telephone monitoring because of the poor fit between means and justifications. The Supreme Court of Montana, in a state case involving the federal wiretapping statute, faulted a telephone company for recording party line conversations for six days to investigate claims of, among other things, obscene phone calls, crass comments, and crackling connections.[358] The Seventh Circuit refused to apply the exception to a telephone company's taping of conversations in an investigation of theft of service.[359] It ruled, however, that the monitoring of certain non-content information fit within the exception.[360] Extrapolating these voice cases to the Internet, no provider should be allowed under this exception to run an unfiltered packet sniffer, capturing complete packets for an extended period of time.

Still, when an ISP is sued or prosecuted for monitoring done in the hot pursuit of an intruder, under these cases it should be given a generously broad reading of the "rights and property" exception. So long as the provider can prove to the court that it had reason to suspect an intruder in the system, the court should find no liability for monitoring, even broad and somewhat indiscriminate monitoring using packet sniffers, in response for a limited time.[361] Complete monitoring to find an intruder for a week seems reasonable; doing it for a month seems pretextual; and monitoring for a year should always be forbidden.

355. Sistok v. Nw. Tel. Sys., Inc., 615 P.2d 176, 180 (Mont. 1980).

356. United States v. McLaren, 957 F. Supp. 215, 219 (M.D. Fla. 1997).

357. *Id.* at 220 ("[T]he interception, recording and subsequent disclosure of complete telephone calls having nothing whatever to do with the cloning fraud under investigation was unreasonable because, obviously, such recordation and disclosure could not possibly be 'necessary' to protect the provider from such fraud.").

358. *Sistok*, 615 P.2d at 182.

359. United States v. Auler, 539 F.2d 642, 646 (7th Cir. 1976).

360. *Id.*

361. Somewhat indiscriminate, because there must still be limits. If a network manager suspects an intruder and monitors a switch carrying the traffic of one thousand users, this probably is more monitoring than is a "necessary incident."

b. "Rendition of Service"

Providers are also entitled to intercept communications as a "necessary incident to rendition of . . . service."[362] With telephone providers, this exception has been rarely litigated and always narrowly construed. It seems to immunize only the overhearing of short conversations by telephone company employees either inadvertently or as a quick check to ensure a line is working.[363] For example, long distance operators have been allowed to remain on a line long enough to ensure a connection has been established.[364] A motel switchboard operator could overhear conversations while performing duties.[365] A telephone company employee atop a telephone pole in response to customer service complaints could attach his device to the line.[366]

ISPs may propose a clever argument about this exception that courts should reject. They may try to strategically characterize the "service" they are rendering. For example, if providers convince courts that they are providing "virus-free web surfing" or "spam-free e-mail," then perhaps they can argue for more leeway to monitor for, respectively, viruses or spam. Taking this argument one more step, providers might argue that the service provided is "ad-subsidized web surfing." This evokes memories of NetZero, a dot-com boom (and bust) company which provided free dial-up Internet access to customers willing to watch ads while they surfed.[367]

The problem with allowing providers to broaden this exception to include such specifically defined services is that it turns on difficult factual questions about how a service is marketed and what customers understand they are buying or receiving, not to mention what types of monitoring are "incident" to the service. All of these questions begin to sound like questions of user consent, but with a twist. While consent, discussed next, focuses on the consent to monitor, "rendition of service" focuses more on the type of service you think you are getting. From a transparency and fairness point of view, the consent argument is more straightforward and better captures the policy interests at stake. Courts should leave the rendition of service interpretation narrow and tightly confined, and push this type of analysis to the consent prong.

362. 18 U.S.C. § 2511(2)(a)(i) (2006).

363. JAMES G. CARR & PATRICIA L. BELLIA, 1 THE LAW OF ELECTRONIC SURVEILLANCE § 3:39 (2008) (summarizing cases).

364. People v. Sierra, 343 N.Y.S. 2d 196, 199–200 (N.Y. Sup. Ct. 1973).

365. United States. v. Savage, 564 F.2d 728, 731 (5th Cir. 1977).

366. United States v. Ross, 713 F.2d 389, 390 (8th Cir. 1983).

367. *See* C. Scott Hemphill, *Network Neutrality and the False Promise of Zero-Price Regulation*, 25 YALE J. ON REG. 135, 173 n.152 (2008) (discussing NetZero).

c. Consent

The other exception that may apply to ISP monitoring is the consent exception.[368] ISPs may lawfully monitor their users without violating the law if and to the extent that their users have previously consented. Consent under the Wiretap Act is very different from ordinary contract law in ways that even seasoned cyberlaw scholars and judges may not initially appreciate. In particular, wiretap consent seems to embrace a form of the proximity principle described in Part III.D.

Wiretap consent may be express or implied, but implied consent is neither a "reasonable expectation of privacy" test, a test of constructive consent,[369] nor a measure of whether the party simply should have known better or had exposed him or herself to some risk of monitoring.[370] Instead, implied consent requires proof that the monitored subject was aware of the monitoring yet continued using the system; the question is, did the user consent in fact?[371] Courts will not, for example, ask what the customer must have known or assess whether the method of notification was reasonably calculated to reach customers.[372] Courts instead ask simply, did this particular user receive notice?

In *Williams v. Poulos*[373] the district court held that an employer violated federal and state wiretap laws when it monitored employee phone calls. Even though the district court found that the CEO had been "told of the 'monitoring' of . . . *employee* telephone calls,"[374] it still found a lack of informed consent because the CEO had not been given enough information to believe that *his* calls were also being monitored.[375] The First Circuit held that without this "minimal knowledge," it would not infer consent.[376]

In *In re Pharmatrak, Inc.*, the First Circuit refused to infer consent from "the mere purchase of a service," particularly when the purchasing parties had insisted no personal data would be collected.[377] In dictum,

368. 18 U.S.C. § 2511(2)(c) (2006) (consent by party to the communication "acting under color of law"); *id.* § 2511(2)(d) (consent by party to the communication "not acting under color of law").

369. *In re* Pharmatrak, Inc., 329 F.3d 9, 19 (1st Cir. 2003); *see* Williams v. Poulos, 11 F.3d 271, 281 (1st Cir. 1993).

370. Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992) ("We do not believe that Deal's consent may be implied from the circumstances relied upon in the Spearses' arguments. The Spearses did not inform Deal that they were monitoring the phone, but only told her they might do so in order to cut down on personal calls."); Potter v. Havlicek, No. 3:06-cv-211, 2007 WL 539534, at *8–9 (S.D. Ohio 2007) (finding no wiretap consent even though monitored person had "utiliz[ed] a computer to which her husband had access and [had used] a 'remember me' feature on her e-mail account").

371. Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998); United States v. Workman, 80 F.3d 688, 693 (2d Cir. 1996); Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990).

372. United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995).

373. 11 F.3d 271 (1st Cir. 1993).

374. *Id.* at 281 (emphasis added).

375. *Id.* at 282.

376. *Id.*

377. *In re* Pharmatrak, Inc., 329 F.3d 9, 20 (1st Cir. 2003).

the court discussed consent in the ISP monitoring situation in particular, indicating that it would interpret ISP contracts closely:

> [S]uppose an internet service provider received a parent's consent solely to monitor a child's internet usage for attempts to access sexually explicit sites—but the ISP installed code that monitored, recorded and cataloged all internet usage by parent and child alike. Under the theory we have rejected, the ISP would not be liable under the ECPA.[378]

There is an even bigger hurdle lurking. ISPs will find it virtually impossible to rely on user consent if they are governed by a state wiretapping law requiring "all party" or "two party" consent. Under such laws, *every* person communicating must have given prior consent. Twelve states require all party consent including Washington, California, and Massachusetts, three states home to many Internet-technology companies.[379]

3. An Entirely Illegal Product Market

Although many of the legal conclusions in this Part have been tentative, one thing can be said with confidence. Tier 1 providers—the providers who run the fastest networks and do not directly serve any users—are almost certainly prohibited under these laws from conducting deep-packet inspection. This is the proximity principle with a vengeance.

Tier 1 providers cannot claim to be using DPI to protect rights and property, because DPI tools are not a "necessary incident" to dealing with the legitimate problems of Tier 1 providers like congestion. It might *interest* a Tier 1 provider to know that 25 percent of the traffic on its network is spam, but how does this interesting tidbit transform into a "necessary" step for protecting the provider's rights and property?

Furthermore, no Tier 1 provider has valid consent from any user to monitor traffic, much less the consent of the tens or hundreds of thousands of users whose communications they are monitoring, even if we put the all party consent issue to the side. None of the monitored users have contracted directly with the Tier 1 provider. Even if some of the users on the network have consented to monitoring by their customer-facing ISP, this will not immunize the out-of-privity upstream provider. Even if consent could be treated like a transitive property, passed along from provider to provider through contract, contracts between ISPs usually say nothing about user privacy or permission to monitor.

Despite the significant limits placed upon a Tier 1 provider under these laws, according to an industry analyst, there are vendors who spe-

378. *Id.* at 21.

379. As of 2003, the states that required the consent of all parties to a communication were California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington. *See* CDT Wiretap Analysis, *supra* note 349, at 11 n.37.

cifically sell DPI to Tier 1 providers.[380] These vendors are selling a product that can never legally be used.[381]

4. Assessing the Law

For the most part, today's wiretap laws strike a reasonable balance between network management and user privacy and incorporate many of the normative principles set out in Part III. Particularly because the wiretap laws are so sweeping and punitive and because the exceptions are muddy and difficult to understand, providers have a strong incentive to avoid venturing away from the status quo. Providers who engage in too much creative monitoring, especially for reasons unrelated to rights, property, and the rendition of service, will probably be sued and may be prosecuted, with the civil verdicts and criminal convictions they suffer serving as cautionary tales to other providers.

B. Amending the Law

Congress should consider an overhaul of all three titles of the ECPA to reflect changes in technology, and to amend away a few glaring inconsistencies. First, to avoid the problems with the envelope analogy, Congress should merge the Wiretap and Pen Register Acts to cover all acts of network monitoring. These laws are very similar to one another, at least in terms of regulating private conduct, and it is both artificial and confusing to treat them dissimilarly.[382] The new unified law should regulate all monitoring—without distinguishing between whether the monitoring is of content or not—provided it is monitoring of data "of or pertaining to a user, customer, or subscriber."

Second, in the merged new law, the "rights and property" and "rendition of service" exceptions should be split into incident response and long-term monitoring exceptions. For "incident response monitoring"—which should be defined as monitoring to protect rights and property, spurred by a triggering event, limited in time, and non-recurring—the new exception should be expansive. In fact, the exception could be made even more forgiving than today's "rights and property" exception by softening the "necessary incident" nexus requirement to a "reasonably re-

380. Light Reading Insider, *supra* note 23.

381. These vendors might even be committing a federal crime merely by selling this technology! Section 2512 of the Wiretap Act makes it a felony to sell a monitoring device "knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications." 18 U.S.C. § 2512(1)(a) (2006).

382. Law enforcement agencies will howl about such a change. The two Acts approach regulating law enforcement court orders in fundamentally different ways. In almost every way, an order to wiretap is significantly more onerous to acquire. Because of this, merging these provisions of the act may be difficult (not to mention politically fraught). Although the value of this distinction is beyond the scope of this Article, for political reasons, if Congress proposes to merge the two acts, it should retain the differences between the law enforcement access provisions at this time.

lated" nexus. Congress should make it clear that the word "reasonably" should be interpreted to incorporate industry standards, and judges should be expected to survey such standards to ensure that the provider is not using the rights and property exception to justify unduly invasive monitoring.

For automated monitoring by routing providers like ISPs, Congress should codify a safe harbor for NetFlow monitoring. A routing provider may capture every piece of information in the NetFlow monitoring set as a matter of course. The risk, of course, is that such a technology-specific law will quickly become outdated. This is probably not a near-term concern, given the long-term history of the protocol and the fact that it is about to be enshrined by IETF in IPFIX.[383] Still, because laws are overhauled infrequently, the law will probably become out-of-date at some point. Thus, Congress should delegate responsibility to a regulator for expanding or contracting this safe harbor. As a model, policymakers should look to the anti-circumvention exceptions provisions of the Digital Millennium Copyright Act (DMCA).[384]

Under the DMCA, it is illegal to circumvent some types of technology used for copyright control.[385] This is why it is likely illegal to copy commercial DVDs, which are protected using a software encryption scheme known as Content Scramble System (CSS).[386] Persuaded that this law might have unintended and undesirable consequences, Congress delegated a triennial review of this prohibition to the Librarian of Congress with assistance from the Register of Copyrights.[387] During this review, which has already occurred thrice, the Librarian is charged with determining whether some people are "adversely affected by the prohibition . . . in their ability to make noninfringing uses."[388] During the last review, the Librarian created new exceptions, among others, for media studies and film professors using film clips in class, and for people unlocking mobile phones to use on a different provider network.[389]

As with the DMCA process, an agency should be given the task of convening every two or three years to consider new expansions to the NetFlow safe harbor of the Wiretap Act. This agency should be charged with considering changes in technology, business needs, and user privacy in deciding whether to expand the list.

383. *See supra* note 296 and accompanying text.

384. 17 U.S.C. § 1201(a)(1)(C) (2006) (instructing Librarian of Congress to engage in triennial review to identify persons "adversely affected" by the anti-circumvention provisions).

385. *Id.* § 1201(a)(1)(A).

386. *See generally* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (discussing CSS and the DMCA).

387. 17 U.S.C. § 1201(a)(1)(C).

388. *Id.*

389. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68472 (Nov. 27, 2006) (to be codified at 37 C.F.R. pt. 201).

Which agency should be charged with this review? The National Institute for Standards and Technology is a good candidate, given its history of national standards setting and its access to subject matter experts.[390] It also is less politicized in many ways than alternatives like the FTC or FCC, and may be seen to have less of a vested interest in the outcome.

What if a provider wishes to collect more than NetFlow information during automated monitoring? The "rights and property" exception should still apply, albeit with the same restrictive "necessary incident" nexus requirement in today's law. Providers will be allowed to aggressively monitor to detect new threats like worms, botnets, and denial of service attacks, but the monitoring they undertake in those efforts must be closely related to the goal pursued.

Third, Congress should overhaul consent. For routing providers, consent should be allowed only on a per-incident basis. Before routing providers can capture information outside the rights and property exception, they must alert users in-band.[391]

Finally, this proposal has focused primarily on collection and not on use and disclosure. Implementing the collection overhaul proposed here would greatly reduce the potential amount of information held by ISPs, which would ameliorate some concerns about use and disclosure. Still, there are reasons why some are worried even about the ISP disclosure and use of the kind of information found in the NetFlow data set. These considerations are beyond the scope of this Article.

V. WHEN NET NEUTRALITY MET PRIVACY

This Article has focused until now on the privacy implications of recent conflicts like Comcast's throttling of BitTorrent.[392] These conflicts, and the Comcast affair in particular, are at the heart of the network neutrality debate. This final Part draws neglected and important connections between privacy and network neutrality.

Network neutrality, or net neutrality, is the principle that ISPs must not treat packets discriminatorily based on content, application, or source.[393] The principle is based on an economic theory of innovation that Tim Wu has called "the evolutionary model,"[394] which holds that the preferred path to innovation is through maximizing the number of poten-

390. *Cf.* NAT'L INST. OF STANDARDS & TECH., FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 197: ANNOUNCING THE ADVANCED ENCRYPTION STANDARD (AES) (2001), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (announcing widely used encryption standard selected by NIST).

391. *See supra* Part III.D.2 (discussing "in band" communications channels).

392. *See supra* Parts II, III.

393. *See* Wu, *supra* note 19, at 168 ("[A]bsent evidence of harm to the local network or the interests of other users, broadband carriers should not discriminate in how they treat traffic on their broadband network on the basis of inter-network criteria.").

394. *Id.* at 145.

tial innovators, leading to a "meritocratic" selection of the winners.[395] This theory is seen to have much in common with the end-to-end principle of computer network engineering: innovation should occur at the "ends" of networks, in the applications running on end user computers, while ISP computers at the "core" should do little more than route packets. This is also referred to as the "dumb network" principle because applications should be smart and the core of the network should be dumb.[396] The three computer scientists who first coined the term have more recently argued that the end-to-end principle maximizes distributed innovation by supporting "the widest possible variety of services and functions, to permit applications that cannot be anticipated."[397]

Mandatory net neutrality has its opponents. They point out that the Internet is inherently non-neutral, because it is built on so-called best effort routing protocols, which make it difficult to avoid delays in the network.[398] Applications that tolerate these problems well (like e-mail) are favored over applications that do not (like VoIP). Neutrality opponents argue that the best way to reduce these problems is to allow providers at the core to innovate, for example, by implementing what is called quality of service, which marks some packets for preferential treatment based on application or source.[399]

A. Flipping the Status Quo

There is a close connection between the network neutrality debate and privacy which to date has received little attention.[400] A provider cannot discriminate between packets without scrutinizing them first. If the ECPA and the state wiretapping laws prohibit ISPs from looking deeply into packets, then certain categories of discrimination will be impossible to accomplish. For example, if a DSL provider is prohibited from using deep-packet inspection to distinguish VoIP packets from other traffic, it cannot block or slow down VoIP. These laws already provide mandatory network neutrality, of a sort, that has never been acknowledged. Because the principles do not overlap perfectly, let us call the principle *network non-scrutiny* (net non-scrutiny) instead.

As providers begin to tiptoe close to the line of discrimination opposed by net neutrality advocates, they will often find themselves tripping over the wiretapping laws first. As plaintiffs' lawyers begin filing class action lawsuits on behalf of customers demanding millions of dol-

395. *Id.* at 145–46.

396. *E.g.*, Richard S. Whitt, *A Horizontal Leap Forward: Formulating a New Communications Public Policy Framework Based on the Network Layers Model*, 56 FED. COMM. L.J. 587, 590 (2004).

397. Thomas W. Chen & Alden W. Jackson, *Commentaries on "Active Networking and End-to-End Arguments*," 12 IEEE NETWORK, May–June 1998, at 66, 70.

398. Kyle Dixon et al., The Progress & Freedom Found., *A Skeptic's Primer on Net Neutrality Regulation* (2006), http://www.pff.org/issues-pubs/pops/pop13.14primer_netneut.pdf.

399. *See id.* at 9–10.

400. *See supra* note 10 (listing articles that have touched on the topic).

lars in remedies for illegal monitoring,[401] and as providers begin losing or settling those suits, they will be forced to abandon entire classes of application and content-based discrimination. Without needing Congress to pass a single law or the FCC to issue a single ruling, net neutrality advocates may find enforceable net neutrality through this unexpected means.

One important result of this analysis is to flip the *status quo ante* in the net neutrality debate. The current assumption is that mandatory network neutrality will result only if proponents convince Congress to enact it.[402] On the contrary, existing legal rules *already* provide network neutrality, at least in the form of network non-scrutiny. The burden of persuasion should be on those who argue in favor of packet discrimination, because to allow deep-packet inspection on a broad scale, the wiretap laws must first be amended.

B. But Is This Really Net Neutrality?

Although privacy concerns overlap with net neutrality goals, the fit is imperfect, and net non-scrutiny does not lead to precisely the results urged by neutrality activists.

First, consider the overlap. As described above, violations of net neutrality are often violations of wiretap law and vice versa. Furthermore, wiretap law allows provider monitoring for the protection of rights and property and the rendition of service. Net neutrality advocates usually allow for similar exceptions to the principle, and the FCC has carved out "reasonable network management" from its principles.[403]

Then again, consider how these goals may diverge. Net neutrality focuses almost exclusively on the *handling* of packets. The worst thing a provider can do is block traffic, and slowing traffic is nearly as bad. Net non-scrutiny, in contrast, focuses instead almost entirely on a provider's *scrutiny* of communications. The worst thing a provider can do is scan and capture the contents of communications. Scrutiny without handling does not violate net neutrality and handling without scrutiny does not necessarily implicate privacy.[404]

Of the four fact patterns discussed in Part I, Comcast's throttling of BitTorrent violates net neutrality the most while AT&T's proposed packet content scrutiny violates net non-scrutiny the most. This is not to say that the two principles are indifferent about the violations that alarm the other. Under net neutrality, AT&T's scrutiny is troubling because it

401. *See* 18 U.S.C. § 2520(c)(2) (2006) (providing statutory damages of $100 per day up to $10,000).

402. *See, e.g.*, *The Future of the Internet: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 110th Cong. 8 (2008) (statement of Lawrence Lessig, Professor of Law, Stanford Law School).

403. Press Release, *supra* note 105, at 2.

404. I say "not necessarily" because "handling" often threatens privacy, even if the provider never saves or archives the information handled. Ross Anderson's example of the once-pregnant woman outed by Phorm is a good example. *See supra* note 219 and accompanying text.

puts in place the architecture for forbidden intelligence and control. Likewise, net non-scrutiny would cast doubt on what Comcast has been doing because in order to throttle BitTorrent, Comcast had to identify communications that looked like BitTorrent. Phorm and NebuAd offend net non-scrutiny because they break down walls between websites and subject users to scrutiny they have never had before. Net neutrality advocates are probably more indifferent about the actions of these companies, so long as they are not discriminating against competitors.

Almost every Internet packet contains one particular header, called the TCP or UDP port, which highlights the difference between the two approaches.[405] The port is a number from zero to 65,535 found near the beginning of the packet.[406] Ports act as sorting mechanisms for incoming messages; applications "listen" only to particular ports, ignoring packets destined for other ports.[407] Web servers typically listen on port 80; outbound e-mail servers on port 25; and inbound e-mail servers often use ports 110 or 143.[408] A wire tapper can scan the port headers of passing packets to quickly and accurately infer the applications being used on the network.

Similarly, the easiest way for a provider to block or throttle an application is to search for packets headed for the port used by the application. Although the technical details are still murky, one way Comcast could have blocked BitTorrent is by blocking packets using ports 6881 to 6900, which are used for many BitTorrent transfers.[409] For this reason, port scrutiny worries net neutrality advocates.[410]

From a privacy standpoint, provider scrutiny of a port is not a great concern. Few applications are so stigmatized or forbidden that knowledge that they are being used alone is a significant privacy breach.[411] Furthermore, ISPs can make convincing arguments that port scrutiny is necessary in reasonable network management. Ports have been logged, for example, in NetFlow from its inception.[412] Tracking traffic by port can help a provider hone down the source of a sudden congestion problem. A spike in port 25 traffic might signal a malfunctioning e-mail server or a spammer. For all of these reasons, port scrutiny is unlikely a wiretap or pen register violation, perhaps to the disappointment of net neutrality advocates.

405. ANDREW G. BLANK, TC/IP FOUNDATIONS 57 (2004).

406. *Id.* at 56.

407. *Id.*

408. *Id.*; ERIC ROSEBROOK & ERIC FILSON, SETTING UP LAMP: GETTING LINUX, APACHE, MYSQL, AND PHP WORKING TOGETHER 164 (2004).

409. WILLIAM VON HAGEN, UBUNTU LINUX BIBLE 16 (2007).

410. Wu, *supra* note 19, at 167–68 (listing discrimination by TCP port as something that might cause concern).

411. In some contexts, peer-to-peer applications or encryption might fall into this category.

412. TechBrief, How Does NetFlow Work?, http://www.netflow-monitor.net/How%20does%20NetFlow%20work.html (last visited Aug. 31, 2009).

This is not a fatal blow to the kinship between non-scrutiny and neutrality, however, because mere port scrutiny will often not prove useful for traffic discrimination due to the evolution of Internet arms races: users can often evade unsophisticated scrutiny by reconfiguring their applications to use non-default ports. For example, during the Comcast-BitTorrent battle, users tried to avoid scrutiny by reconfiguring their BitTorrent clients to use a non-standard port.[413] If this had been successful, Comcast would have had to scrutinize other, deeper parts of packets, exposing themselves to potential wiretap liability. Arms races tend to push ISPs to deeper parts of packets, thus bringing net neutrality and privacy advocates closer together.

As it turns out, Comcast probably did much more than just look at port numbers. Researchers have reported that Comcast had been blocking other protocols such as Gnutella and Lotus Notes in addition to BitTorrent.[414] These applications use different port numbers, but they all exhibit similar traffic patterns. In fact, some users reported throttling of encrypted BitTorrent traffic, suggesting that Comcast had been using particularly sophisticated monitoring techniques.[415] One company that has emerged as a likely partner is Sandvine.[416] Sandvine is a DPI vendor that sells products that scrutinize packets much more deeply than the port.[417]

In a sense, net non-scrutiny gives the ISP one bite of the apple. ISPs may scrutinize (and thus discriminate) between packets so long as the level of scrutiny is low, which may work before the arms race has begun. But once low scrutiny fails to work—because users have started using counter-measures—providers lose the ability to discriminate legally.

C. Resituating the Net Neutrality Debate

The final important contribution of this Article is to resituate the net neutrality debate. Proponents of neutrality argue solely about its benefits for innovation and economic growth.[418] Sometimes, they clothe these arguments in the language of "freedom," but by this they mean a

413. *See* Ekr, *Traffic Blocking Evasion and Counter-Evasion*, EDUCATED GUESSWORK, Oct. 29, 2007, http://www.educatedguesswork.org/movabletype/archives/2007/10/traffic_blockin.html.

414. PETER ECKERSLEY ET AL., PACKET FORGERY BY ISPS: A REPORT ON THE COMCAST AFFAIR 5 (2007), http://www.eff.org/files/eff_comcast_report2.pdf.

415. Ernesto, *supra* note 93.

416. Ben Popken, *Damning Proof Comcast Contracted to Sandvine*, THE CONSUMERIST, Oct. 27, 2007, http://consumerist.com/consumer/bittorrent/damning-proof-comcast-contracted-to-sandvine-315921.php.

417. Sandvine Inc., Solutions Overview, http://www.sandvine.com/solutions/default.asp (last visited Aug. 31, 2009).

418. *E.g.*, Wu, *supra* note 19, at 166–67; Brett M. Frischmann & Barbara van Schewick, *Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo*, 47 JURIMETRICS 383, 389–92 (2007); *see also* Christopher S. Yoo, *Network Neutrality and the Economics of Congestion*, 94 GEO. L.J. 1847, 1851 n.13 (2006) (noting that "network neutrality proponents defend their proposals almost exclusively in terms of the economic benefits of innovation").

narrow, market-drenched conception of freedom.[419] By shifting the focus from innovation to privacy, this Article reconceives net neutrality as being about more significant and profound freedoms. If ISPs are permitted to set up systems that peer into and store the full-packet content of communications on their networks, not only will they be able to discriminate, but also they will be able to scrutinize. An architecture of discrimination is an architecture of surveillance, one that can be lent out to intelligence agencies, copyrighted content owners, and subpoena-wielding civil litigants to reveal everybody's deepest secrets.[420] A neutral network is a more private network.

The debate has taken place almost exclusively on insular economic terms. All of the values lined up on both sides are internal to this economic frame. These are particularly vexing economic questions, because they require predicting the effect of complex inputs on a complex industry dominated by new technology, and the net neutrality debate has devolved into a bare-knuckles economics brawl. Advocates on both sides argue over the necessary preconditions for innovation, and they debate whether some types of innovation are better than others.[421] Neither side has landed a knock-out punch, however, and both sides admit that their predictions might be wrong.[422]

Thus, Professors Philip Weiser and Joseph Farrell discuss how firms might "internalize complementary efficiencies."[423] Professor Christopher Yoo criticizes net neutrality by surveying the economic theory of congestion pricing and devising what he calls "network diversity."[424] Professors Brett Frischmann and Barbara van Schewick rebut Yoo's theories.[425]

Recasting the debate as one about the proper levels of privacy makes an intractable debate tractable. Privacy brings in an entirely different frame of reference, one composed of values that have nothing to do with innovation and economic prosperity. Stacked up against privacy, there is more space between competing visions of ISP behavior: doing X might make it difficult to deploy next-generation video applications, but it will protect user privacy in return. It will be easier to compare the significance of one value versus another. It will be easier to make predictions about the political outcomes. In this case, there is virtue in comparing apples to oranges.

419. BEN SCOTT ET AL., WHY CONSUMERS DEMAND INTERNET FREEDOM: NETWORK NEUTRALITY: FACT VS. FICTION 3 (2006), http://www.freepress.net/files/nn_fact_v_fiction_final.pdf.

420. *See* ZITTRAIN, *supra* note 256, at 116–17.

421. *See supra* note 418 and accompanying text; *see also* Joseph Farrell & Philip J. Weiser, *Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age*, 17 HARV. J.L. & TECH. 85 (2003).

422. *See supra* note 421.

423. Farrell & Weiser, *supra* note 421, at 101.

424. Yoo, *supra* note 418, at 1851, 1863–74.

425. Frischmann & van Schewick, *supra* note 418.

Privacy also draws in institutions and experts who have been sidelined thus far in the net neutrality debate. Although net neutrality debates take place most often in the FCC and the competition-centric sides of the FTC and DOJ, a debate about privacy will draw in other governmental entities like Homeland Security, the FBI, the criminal and national security sides of DOJ, and the privacy side of the FTC.

Wiretap law will also draw the courts into the neutrality debate for the first time in ways that can be very helpful. Although legislatures and regulatory agencies should be making the sweeping decisions about network neutrality for both legitimacy and institutional competency reasons, these branches of government are clumsy at gathering facts about the evolution and legitimacy of network management techniques. The FCC held two public hearings arising from Comcast's decision to throttle BitTorrent. At the first, Comcast tried to influence the tenor of the debate by paying people to fill seats which otherwise might have been occupied by vocal critics.[426] At the second hearing, Comcast refused to participate at all.[427]

In court, providers will be forced to participate in discovery, revealing facts in much more detail and with much greater accuracy. Further, they will be forced to focus on particular techniques rather than provide platitudes about network management writ large. Then, after the facts are revealed, engaged advocates fighting over real stakes will defend their practices before a neutral judge. Of course, litigation should not replace or delay the broader political debate, and such cases and legislative deliberations should operate in parallel, providing feedback to one another.

Expanding the net neutrality debate will also draw in activists on both sides who have watched quietly thus far. The Electronic Frontier Foundation (EFF), for example, has mostly sat out the debate (although their technical work on the Comcast throttling was foundational). EFF might not be able to resist getting more involved if the focus shifts to privacy, one of their two key issues (the other being Copyright law), and they should have much to say about the question of ISP monitoring. Another noticeably quiet voice has been the Electronic Privacy Information Center (EPIC). On the other side, the copyrighted content industries will see privacy-justified restrictions on ISP monitoring as threats against tools they could use to protect their intellectual property. Granted, quantity is not quality, and increasing the number of participants may just make the debate noisier and more complex. Still, with issues as important as these, including more participants in the debate can help ensure that regulations avoid unintended consequences.

426. Bob Fernandez, *Comcast Paid to Fill Seats at FCC Hearing*, PHILA. INQUIRER, Feb. 28, 2008, at A1.

427. Stefanie Olsen, *Absent Comcast in Hot Seat at FCC Hearing*, CNET NEWS, Apr. 17, 2008, http://news.cnet.com/8301-10784_3-9921945-7.html.

Introducing privacy reinvigorates the network neutrality debate, which until now has been a single-minded debate about innovation but has devolved into a bare-knuckled, intramural, economics brawl. Privacy expands the debate into a broader discussion of freedom, liberty, and autonomy. It offers more meaningful choices between alternatives, and it makes the intractable tractable.

CONCLUSION

Because ISPs pose such a high risk of terrible harm to so many people, and because of the unmistakable signs that things are getting worse, they must be regulated. The ECPA already regulates ISP monitoring, and although it does so imperfectly and shrouded in too much complexity, it embodies most of the principles and theories developed in Part III. The ECPA likely forbids many invasive forms of ISP monitoring, and this Article predicts a series of class-action lawsuits and, possibly, criminal prosecutions for the worst offenders. If ISPs exercise restraint and respect their past promises of privacy, they can avoid the pain and headaches of litigation and forestall new forms of even more restrictive regulation.

Finally, this Article aims to serve as a model for dismantling a technology law stovepipe, to borrow a term from the national security and intelligence worlds. Intelligence agencies have been criticized for collecting information insularly without sharing enough between agencies, maintaining the information in metaphorical "stovepipes."[428] Technology law specialists—practitioners and scholars alike—also construct stovepipes of knowledge, dividing themselves into specialties like telecommunications law, intellectual property, and information privacy, to name only three. Too often, problems are examined from the vantage point of only a single specialty, rather than through the lenses of more than one of these. This can blind us to solutions visible only by breaking down these somewhat artificial barriers.

In particular, debates about ISP behavior might seem intractable when viewed solely within the telecommunications law or information privacy stovepipe. But when viewed through both of these points of view simultaneously, better answers are visible. In particular, once we recognize that the network neutrality debate is about more than just innovation and telecommunications policy, we will finally see the path to resolution.

428. STAFF OF H. COMM. ON INTELLIGENCE, 104TH CONG., IC21: THE INTELLIGENCE COMMUNITY IN THE 21ST CENTURY 7–8 (Comm. Print 1996).