THE RISE AND FALL OF INVASIVE ISP SURVEILLANCE

PAUL OHM*

ABSTRACT

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 them to put their users' secrets up for sale, and judging from a recent flurry of reports, ISPs are giving in to the temptation 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 proposes an innovative new theory of communications privacy to help policymakers strike the proper balance between user privacy and ISP need. We cannot simply ban aggressive monitoring, because ISPs have legitimate reasons for scrutinizing communications on an Internet teeming with threats. Using this new theory, policymakers will be able 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. Thanks to Orin Kerr, Peter Swire, and Phil Weiser for comments. Early versions of this paper were presented to the Privacy Law Scholars 2008 Conference and the Computers, Freedom, and Privacy '08 conference. I thank all of the participants and my colleagues for their comments, and in particular Brad Bernthal; Aaron Burstein; Bruce Boyden; John Chapin; Samir Chopra; Danielle Citron; Will DeVries; Susan Friewald; Jon Garfunkel; Dale Hatfield; Stephen Henderson; Chris Hoofnagle; Derek Kiernan-Johnson; Scott Moss, Deirdre Mulligan; Frank Pasquale; Wendy Seltzer; Sherwin Siy; Gerard Stegmaier; and Tal Zarsky.

Electronic copy available at: http://ssrn.com/abstract=1261344

INTRODUCTION

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

New threats to privacy on the Internet do not want for academic attention. Scholars have discussed the threat to privacy from Google,[2] data

[1] This Article defines Internet Service Providers (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 or 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.B.2.b.

[2] James Grimmelmann, *The Structure of Search Engine Law*, 93 IOWA L. REV. 1, 17-23, 39-41, 56-58 (2007).

Electronic copy available at: http://ssrn.com/abstract=1261344

aggregators,[3] hackers,[4] spyware authors,[5] identity thieves,[6] and the government,[7] but they have said nothing about the threat from ISPs. In contrast, regulators and legislators have focused with great interest on ISP monitoring,[8] and the media has covered the topic extensively.[9] This Article fills a conspicuous void in legal scholarship, providing a complete accounting of the potential threat to privacy from ISP monitoring.

A potential threat to privacy, however, is not the same thing as a likely invasion, and this Article provides the tools for distinguishing one from the other. In this case, the evidence points in opposite directions: on the one hand, ISPs have a track record for respecting user privacy. On the other hand, technological hurdles that have prevented providers from monitoring invasively have recently fallen.

To resolve this contradiction, Part I, which is both descriptive and predictive, explores the history, evolution, and nature of ISP surveillance. Online wiretapping used to be easy, then it became difficult, and today it is easy again. This Article quantifies this conclusion, importing data and methodologies from computer hardware engineering that have never before appeared in legal scholarship.

As technological barriers have fallen, spurring the disintegration of user privacy, markets and norms have done nothing to halt the trend. The market has placed extraordinary pressures on ISPs to find new sources of revenue. Advertisers and copyright owners have risen to meet this need, offering ISPs great sums in return for their users' secrets. The norms and ethics of network monitoring are full of gray areas and differences of opinion, so ISPs face little fear of social sanction from their engineering peers.

Given this confluence of technological, economic, and ethical forces, this Article forecasts a coming storm of unprecedented, invasive ISP monitoring. Specifically, ISPs will embrace the use of what are known as deep-packet inspection (DPI) tools; their use of these tools will lead to the greatest reduction of user privacy in the history of the Internet, and users will suffer dire harms. Part I concludes that ISP monitoring must be regulated.

---

[3] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE *passim* (2003) [*hereinafter* SOLOVE, DIGITAL PERSON].

[4] BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD (2004).

[5] Paul M. Schwartz, *Privacy Inalienability and the Regulation of Spyware*, 20 BERK. TECH. L.J. 1269 (2005).

[6] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227 (2003).

[7] Orin S. Kerr, *Internet Surveillance After the USA PATRIOT Act: The Big Brother that Isn't*, 97 N.W.U.L. REV. 607 (2003).

[8] *See* Part I.B.3 (describing four conflicts surrounding ISP monitoring and government responses to each).

[9] *E.g.*, Ellen Nakashima, *Some Web Firms Say they Track User Behavior Without Explicit Consent*, WASH. POST, Aug. 12, 2008 at D1; Stephanie Clifford, *Web Privacy on the Radar in Congress*, N.Y. TIMES, Aug. 10, 2008; Peter Kaplan, *FCC Orders Comcast to Modify Network Management*, WASH. POST, Aug 1, 2008; Saul Hansell, *I.S.P. Tracking: The Mother of all Privacy Battles*, N.Y. TIMES, March 20, 2008.

In a search for the proper shape of this regulation, Part II proposes a new theory of communications privacy. It first exposes flaws in the analogy usually used to model the interception of communications: the sealed envelope with private contents on the inside and non-private addressing information on the outside. As a metaphor for Internet communications, the envelope analogy is overinclusive, underinclusive, and question-begging.

Instead, the Article adopts and extends the theory of contextual integrity, which protects privacy according to pre-existing norms. While embracing the general contours of this theory, the Article criticizes the group of writers from which the theory emanates—the so-called New Privacy Scholars. These writers have discussed the privacy-security balance only from one side of the scale, arguing that privacy is much more fundamental than people have realized. Instead of elevating privacy, these arguments have made privacy seem more abstract and detached from the type of harms that galvanize the public and policymakers. This Article shifts the scrutiny to the other side of the scale, casting a skeptical and critical eye at arguments for less privacy. In particular, this Article demonstrates how arguments about security and necessity tend to be exaggerated.

Applying this theory, Part III critiques the three most-often heard defenses of invasive monitoring. First, Subpart A establishes that ISPs exaggerate their ability to avoid privacy harms by anonymizing the data they collect. Next, Subpart B tackles the complex technical question of ISP need. Provider assertions of the need to monitor user communications more deeply and thoroughly than they have in the past do not hold up to close scrutiny. This discussion represents the first comprehensive discussion of "reasonable network management," what the Federal Communications Commission (FCC) calls the line between permissible and impermissible provider techniques.

Finally, Subpart C points out the tenuousness of ISP claims that they have user consent to monitor expansively. It proposes a new theory of consent that weighs and categorizes the relationship between a provider and its users to decide if consent should be allowed. Some providers should be able to obtain consent more easily than others, based on what the Article calls their *proximity* to users. Non-proximate providers should never be allowed to monitor with supposed consent.

Part IV turns from an examination of regulation in the abstract to a survey of existing law. Regulators need not regulate anew to prevent the worst ISP monitoring abuses, because these acts are probably already illegal under the American wiretapping laws. Although these laws have rarely been invoked against ISPs in the past, this Article expects that lawsuits challenging new ISP techniques will be filed much more often.

Finally, this Article's sustained focus on ISP behavior invites comparisons to the network neutrality debate, a debate about who should control innovation on the Internet. This debate has been at times engrossing and fundamentally important, and more recently, stagnant and frustrating. It has also attracted a surprising amount of attention from the public and politicians, who have been deeply engaged in discussions about ISP

behavior and the sources of online innovation. In Part V, this Article connects the wiretapping laws to the network neutrality debate, something nobody else has done.[10] If providers 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.

Introducing privacy reinvigorates the network neutrality debate, henceforth a single-minded debate about innovation, which 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.

I. PRIVACY ONLINE AND HOW IT IS LOST

Not a week seems to go by without a report of a new form of invasive ISP monitoring.[11] These reports mark a significant change from a longstanding industry tradition of respect for customer privacy. Subparts A and B relate some of these stories and offer an explanation for the sudden change. The most important driver is technological change. Wiretapping online used to be difficult and today it is easy, as a survey of a few principles from the field of computer architecture will demonstrate. New forms of ISP surveillance will harm users in significant ways, described in Subpart C, and the Part concludes that regulators must ban at least the most invasive forms of ISP monitoring.

A. A Brief History of Internet Surveillance

This is a story of restraint and constraints. ISPs have monitored with restraint, but only because they have been constrained by inferior tools.

1. Restrained: Heavily Filtered for Narrow Purposes

At least since Congress first regulated telephone wiretapping and up to the present day, telephone companies have respected subscriber privacy. Although these companies have always had the technology to listen to and record conversations, they have tended to listen only when they have been checking the line, investigating theft of services, assisting law enforcement, or after receiving the express, time-limited consent of the speakers.[12] Providers caught recording in other circumstances have been punished

[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. Rob Frieden, *Internet Packet Sniffing and its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 633 (2008). Also, several non-academic commenters have explored similar points of view. Daniel Berniger, Forget Neutrality—Keep Packets Private, GigaOm blog, Jan. 14, 2007, 8:30 PM PST, http://gigaom.com/2007/01/14/forget-neutrality-keep-packets-private/; 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.

[11] *See* Part I.B.3 for a summary of recent stories.

[12] *See infra* Part IV.A.2.

severely for illegal wiretapping.[13] This is a pillar of the concept of "common carriage."[14]

At the same time, largely in line with federal legislation,[15] regulation,[16] and Supreme Court case law,[17] telephone companies have routinely collected the non-content information relating to telephone calls: principally who called whom and for how long. The line between permissible and impermissible telephone monitoring has been drawn using 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.

Once these and other providers began providing access to the Internet, they could have redrawn the lines of customer privacy. For one thing, the envelope analogy has proved very difficult to apply online, because the concepts of content and non-content tend to get jumbled on the Internet.[18] Also, Internet providers have fought to exclude themselves from the "common carriage" label, and for the most part, have managed to shake off most of the burdens of that designation.[19] Still, 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. From the dawn of the commercial Internet in the mid-1990s until the very recent past, ISPs had respected user privacy, tracking communications in a broad way but not in a deep way.

ISPs have used two methods for monitoring user communications. 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 automated monitoring for five reasons: to gauge the health of the network, secure the network, detect spam, detect viruses, and police bandwidth.[20] Automated monitors tend to

---

[13] *See infra* Part IV.A.1.

[14] *Cf.* 47 U.S.C. § 222 (imposing privacy restrictions on common carriers).

[15] *Compare* 18 U.S.C. § 2511(1)(a) (subjecting those who intercept the "contents of 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 (permitting limited use for marketing of certain information relating to a customer's telephone services).

[17] *Compare* U.S. v. Katz, 389 U.S. 347, 353 (1967) (prohibiting use of recording device to monitor telephone call) *and* Berger v. New York, 388 U.S. 41, 58-60 (1967) (requiring heightened procedural requirements in order for the government to obtain an order to wiretap) *with* 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).

[18] *See infra* Part II.A (discussing the poor fit between the envelope analogy and Internet technology).

[19] James B. Speta, *A Common Carrier Approach to Internet Interconnection*, 54 FED. COMM. L.J. 225, 248 (2002).

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

ignore content and other information packed, to use another common metaphor, "deeply" within packets.

In contrast, ISPs turn to targeted monitoring to respond to incidents. When a network engineer suspects trouble on the network[21]—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. Packet sniffers rarely scrutinize the data of many users, because they are often deployed at points in the network where the information of only a few users can be seen and collected.

An ISP's mix of automated and targeted monitoring dictates the level and type of privacy a user enjoys. Automated monitoring protects privacy by "forgetting" much more than it remembers, 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. Although automated computer programs had screened most of their Internet activity, almost all of the private details had been discarded, never to be viewed by human eyes. Why did users once enjoy this much privacy, and what has changed?

2. Constrained: Technological Barriers to Invasive Monitoring

Professor Larry Lessig has identified four regulators of online conduct—markets, norms, law, and technology.[22] Each of these has helped restrict the frequency and invasiveness of ISP monitoring, but technology has played the pre-eminent role. Users have enjoyed privacy because the devices that monitor networks have been unable to keep up with the amount of data crossing networks.

a) The Present-Day Impossibility of Complete Monitoring

The simplest, most effective, and most privacy invasive, form of network monitoring would be one combining aspects of the automated and targeted monitoring techniques, storing every packet crossing a network forever. I will return repeatedly to this possibility, which I call the *complete monitoring* solution. A provider that could completely monitor its network could achieve every goal imaginable—from the benign to the terrifying.

Complete monitoring has always been impossible for high-speed networks because computers have lacked the horsepower to analyze and capture information quickly enough. 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 filter every single packet passing across their network than the Post Office is able to

[21] 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.

[22] LAWRENCE LESSIG, CODE VERSION 2.0 at 5 (2d ed. 2006)

open every envelope."[23] 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."[24]

Why is complete monitoring impossible? Picture network monitoring like a police officer on the side of a road, watching the traffic going by, looking for drivers swerving or speeding or for cars with outdated license plates. The two metrics that determine whether the officer can inspect every car are 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. Slow, old computers analyze and store data slowly, and fast, new computers work quickly. Likewise, 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.

Not too long ago, complete monitoring was impossible because the roads were too wide and the police officers too dim. Through fast network connections once flowed more data than slow computer processors could analyze and store.[25] Some simple, back-of-the-envelope calculations, however, should lead us to wonder whether these facts have always been the case, and more ominously, whether they might no longer be true in the near future. According to these calculations, providers may soon have the capability to conduct complete monitoring, which would have a terrifying and profound impact on user privacy.

b) The Race Between Processors and Bandwidth

Rather than freeze the scene at one moment in time, let us take a dynamic view and 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 better be 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 fail at his job. If we upgrade both the road and the officer, then whether the surveillance will succeed depends on the relative rates of improvement.

The last scenario—of simultaneous improvement—describes the evolution of network monitoring. Over the past twenty-five years, both the speed of residential network connections and the power of monitoring

---

[23] BBC, *Illegal Downloaders 'Face UK Ban'*, BBC NEWS, Feb. 12, 2008, http://news.bbc.co.uk/2/hi/business/7240234.stm.

[24] Eleanor Dallaway, *Music Piracy Born Out of a 'Something for Nothing' Society*, INFOSECURITY-MAGAZINE.COM, April 2008, http://www.infosecurity-magazine.com/features/April08/Piracy.html.

[25] *See generally* Rob Fixmer, *Personal Computers: Phone Companies Create Traffic Jam on Road to Internet*, N.Y. TIMES, Sept. 1, 1998, available at http://query.nytimes.com/gst/fullpage.html?res=9F02E6DF143FF932A3575AC0A96E958260.

hardware have significantly increased. They have increased at differing rates, however, and 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.

(1) Personal Computer to Pre-Commercial Internet

In 1984, personal computers were still in their infancy, but users were already connecting them to one another with computer modems, using them to dial bulletin board systems to use message boards and transfer files.[26] At the time, the fastest consumer modem was the Hayes Smartmodem 1200, so-named because it could send or receive 1200 bits of data per second.[27] At that rate, it would have taken nearly three hours to download the text of the Bible.[28]

Suppose the telephone company of 1984 had decided to monitor all of the bits traveling to and from all of its customers' computers over its telephone 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.[29] A common metric for comparing processing power across processors is MIPS, for millions of instructions per second, and the 80286 could calculate 1.5 MIPS. A computer cannot do real work with a single instruction—which is a very primitive operation such as "compare bit A with bit B to see if they are equal"—so as a very rough estimate, let us assume a processor needs twenty instructions to monitor a single bit of modem data (perhaps a few instructions to load the data from the telephone line into memory, a few for moving the data around in memory, and a few for pushing the data into the output queue).

Because modem rates and MIPS both measure rates per second, they can be compared directly to one another. A single PC AT, working at full capacity on this task, could analyze all of the data from 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.[30]

Providers would maintain the advantage in the monitoring arms race for at least another decade and a half, as modem manufacturers innovated

---

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

[27] Tony Messina, *Review—Hayes Smartmodem 1200*, ANALOG COMPUTING (1983), *available at* http://www.cyberroach.com/analog/an19/hayes_1200.htm.

[28] The zip file version of the King James Bible downloadable from the Project Gutenberg archive measures 1.59 megabyte. Project Gutenberg, The Bible, King James Version, Complete Contents, http://www.gutenberg.org/etext/7999 (last visited July 27, 2008).

[29] Old-Computers.com, IBM PC AT, http://www.old-computers.com/museum/computer.asp?c=185 (visited July 17, 2008).

[30] 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.

slowly while processors continued along the torrid pace of progress predicted by the famous exponential curve known as Moore's Law.[31]

(2) Dawn of the Commercial Internet to Today

Let us jump ahead fifteen years. In 1997, customers began using cable modems to access the Internet,[32] for the first time, enjoying an exponential gain in bandwidth, to speeds approaching three megabits or million bits per second.[33] At this rate, it would have taken only four seconds to download the Bible.

Meanwhile, in 1997, Intel's fastest processor was the Pentium II, rated at 300 MIPS.[34] 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. 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.

(3) The Legacy of the Late 90's

Before we continue these calculations to the present, let us pause to reflect on the year 1997, which fell within an incredibly important era in the history of the Internet, not only for the rollout of residential broadband. The Internet boom was in full swing, and users were signing on in unprecedented numbers. Compared to the kind of users who had signed on in 1983, however, the 1997 users were less technically savvy and less aware of the informal rules of etiquette that once governed the net. 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.[35]

In 1997, not only would ISPs have liked to monitor these vast hordes of clueless users, but also another related and even more serious risk loomed. Malcontents—spammers and virus and worm authors—were said to have been attracted, like flies to honey, to the clueless hordes and their always-on broadband connections.[36] Providers must have feared daunting new threats on the network. At precisely this moment of both incredible

---

[31] *See infra* Part I.B.1 (discussing Moore's Law).

[32] 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.

[3333] JONATHAN E. NEUCHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 141-43 (2005) (describing cable modem service).

[34] Marshall Brain, How Microprocessors Work, HowStuffWorks, http://computer.howstuffworks.com/microprocessor1.htm (last visited August 3, 2008).

[35] Eternal September was coined in 1993 when America Online first allowed its millions of users to have access to parts of the Internet. Jargon File, entry for "September that never ended," http://www.catb.org/jargon/html/S/September-that-never-ended.html.

[36] 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).

growth and unprecedented new fears, the calculations presented above establish that providers would have found it difficult to monitor the masses with ease.

We began with a search for root causes of our online privacy. 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-1990's, 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.

The era has had an enduring technological legacy. Two of the most widely used packet sniffers[37] were released at in the 1990's, Ethereal (now Wireshark) in 1998[38] and dsniff in 1999.[39] One of the most important automated monitoring protocols, NetFlow, was first released in 1996.[40] Ethical rules for monitoring were probably also developed during this time of imbalance in favor of bandwidth over processors. We enjoy the privacy we have today in large part because a decade ago, providers could not take it away.

B. Changes

1. Evaporating Technological Constraints

Let us continue our march through history. Today, a decade from where we left off, we are witnessing the first order-of-magnitude bandwidth gain since the dawn of the cable modem. Verizon now offers their FiOS fiber optic service to the home and already claims 1.8 million subscribers.[41] The fastest FiOS connection sold today delivers a blistering fifty megabits downstream.[42] Cable companies promise that a new kind of cable modem—based on a standard called DOCSIS 3.0—will deliver up to fifty megabits downstream as well.[43] Over such a connection, the Bible can be downloaded in less than a quarter-of-a-second.

---

[37] Insecure.org, Top 11 Packet Sniffers, http://sectools.org/sniffers.html (last visited July 27, 2008). The venerable tcpdump is older, first released in 1988.

[38] Wireshark, About Wireshark, http://www.wireshark.org/about.html (last visited July 27, 2008).

[39] Larry Loeb, On the Lookout for dsniff, http://www.ibm.com/developerworks/library/s-sniff.html (Jan 1. 2001). Another popular tool, ettercap, was first released in 2001. Ettercap History Page on SourceForge.net, http://ettercap.sourceforge.net/history.php (showing initial release date January 25, 2001).

[40] NetFlow is discussed in great length *infra* Part III.B.4.b.

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

[42] Eric Bangeman, *Verizon, Comcast Pump up the Bandwidth. Where's AT&T?*, ARS TECHNICA, May 10, 2007, 10:38 PM http://arstechnica.com/news.ars/post/20070510-verizon-comcast-pump-up-the-bandwidth-wheres-att.html (claiming theoretical FiOS speeds up to 400 megabits after system upgrade).

[43] Brad Stone, *Comcast to Bring Speedier Internet to St. Paul*, N.Y. TIMES BITS BLOG, April 7, 2008, http://bits.blogs.nytimes.com/2008/04/02/comcast-to-bring-speedier-internet-to-st-paul/; Bangeman, *supra* note 42 (noting DOCSIS 3.0 demonstration speed of 150 megabits).

Meanwhile, Intel's fastest consumer processor, the Core2Extreme, rates just shy of 60,000 MIPS. 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. Thus, despite the order of magnitude increase in bandwidth, processors have done much better than keep up, and providers today can monitor 60,000,000,000 / (20 * 50,000,000) = 60 FiOS connections, about the same ratio they enjoyed between the PC AT and the Hayes Smartmodem in 1983.

This is an interesting trend: 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 co-founder 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.[44] Others claim the doubling occurs every eighteen months.[45]. Roughly speaking, 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 the other informal, suggest that the growth in the rate of residential bandwidth is similar to Moore's Law and perhaps a bit 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.[46] At around that time, a web usability expert, Jakob Nielsen predicted in 1998 that a high-end user's bandwidth grows 50% per year,[47] slower than the eighteen-month version of Moore's Law, leading him to conclude that, "bandwidth grows slower than

---

[44] Moore's law traces back to a 1965 magazine article by 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 MAGAZINE, April 19, 1965 ("The complexity for minimum component costs has increased at a rate of roughly a factor of two per year."), available at http://download.intel.com/research/silicon/moorespaper.pdf.

[45] *See* Tom R. Halfbill, *The Mythology of Moore's Law*, IEEE SOLID-STATE CIRCUITS SOCIETY NEWSLETTER (Sept. 2006) 21 (seeking to correct misconceptions about Moore's Law), available at http://www.ieee.org/portal/cms_docs_societies/sscs/PrintEditions/200609.pdf.

[46] Charles A. Eldering, Mouhamadou Lamine Sylla, & Jeffrey A. Eisenach, *Is There a Moore's Law for Bandwidth?*, IEEE COMMUNICATIONS MAG., Oct. 1999, http://ieeexplore.ieee.org/iel5/35/17246/00795601.pdf. . *See also* Steven Cherry, *Edholm's Law of Bandwidth*, IEEE SPECTRUM (July 2004) (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).

[47] Jakob Nielsen, Nielsen's Law of Internet Bandwidth (April 5, 2008) (updated 2008), http://www.useit.com/alertbox/980405.html.

computer power."[48] 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, but will other constraints—such as norms or the market—step in to fill the void?

2. Extraordinary Pressures

a) Pressure to Upgrade Infrastructure and Obtain ROI

ISPs are struggling for survival.[49] Many economists say the deck is stacked against them.[50] 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. The result, as one industry analyst puts it, is "accelerated erosion of the revenue earned per bit."[51]

Broadband ISPs have responded by searching for new sources of revenue. To this end, they have recognized the emerging market for trading user privacy for cash, which Google has proved can be a very lucrative market.

b) Google Envy and the Pressure to Monetize

Providers have what some have called "Google envy."[52] Google has demonstrated how to grow rapidly by "monetizing" user behavior, in their case by displaying advertisements matching a users' recent search queries.[53] Google's success has redefined expectations for both profitability and

---

[48] *Id.* In 2000, George Gilder predicted that the total bandwidth of the entire network would double every six months. This prediction inspired Gilder to speculate about a world of infinite bandwidth. GEORGE GILDER, TELECOSM: HOW INFINITE BANDWIDTH WILL REVOLUTIONIZE OUR WORLD (2001). 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.

[49] Susan Crawford, *The Ambulance, The Squad Car, and the Internet*, 21 BERK. TECH. L.J. 873, 877-78 (2006) (describing woes of telephone companies in part from competition from VoIP).

[50] *See* DELOITTE TOUCHE TOHMATSU, TELECOMMUNICATIONS PREDICTIONS: TMT TRENDS 2007, 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.").

[51] Light Reading Insider, Deep Packet Inspection: Vendors Tap into New Markets, http://www.lightreading.com/insider/details.asp?sku_id=1974&skuitem_itemid=1060 (executive summary for analyst's report) (last visited August 3, 2008).). *See also* DELOITTE TOUCHE TOHMATSU, *supra* note 50, at 7.

[52] Raymond McConville, Telcos Show Their Google Envy, April 8, 2008, http://www.lightreading.com/document.asp?doc_id=150479&f_src=lightreading_FinancialContent.

[53] *Id.*

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.

Furthermore, this pressure has come at a time when IT was already being transformed to be more "aligned with business interests," to use an oft-heard phrase.[54] Senior managers strive to "run IT more like a business,"[55] for example assigning two managers to each IT project, one versed in IT, the other in business; adapting techniques developed for making investments for setting IT priorities; and rotating IT staff through other departments like finance.[56] After expending all of this energy making IT run like a business, it is natural for managers to try to turn IT into a profit center,[57] and the easiest way to do that is by learning from Google and monetizing behavioral data at the expense of user privacy.

c) All-you-can-eat Contracts and Network Congestion

Another way 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 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.

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

---

[54] "However, there is a significant movement in the industry to align IT with the business initiatives of organizations. In order to move from component level monitoring to service level monitoring it is necessary to elevate above the device level." OpenWater Solutions, LLC, FCAPS—Is It Enough?, http://www.openwatersolutions.com/fcaps.htm (last visited August 3, 2008).

[55] Business Management, How To: Align IT with Business Goals, http://www.busmanagement.com/currentissue/article.asp?art=27050&issue=165.

[56] Thomas Hoffman, *Corporate Execs Try New Ways to Align IT with Business Units*, Oct. 27, 2003, COMPUTERWORLD, http://www.computerworld.com/managementtopics/management/story/0,10801,86466,00.html.

[57] Business Management, Turning IT into a Business Center, http://www.busmanagement.com/currentissue/article.asp?art=272456&issue=235; IT Business Edge, Hey IT, Work Hard to get Requirements Right, http://www.itbusinessedge.com/item/?ci=21942, Nov. 14, 2006 (quoting Theresa Lanowitz, "Rather than being an additional appendage, [IT] needs to be brought into the business so that the IT people really understand what is happening in line of business and can make IT part of the profit center of a company instead of a cost center."); Richard L. Routh, *5 Tips on IT Alignment that can Generate Profit*, CIO, April 11, 2008, http://www.cio.com/article/333713/_Tips_on_IT_Alignment_That_Can_Generate_Profit.

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 p2p networks.[58]

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 Congress to enact the Communications Assistance for Law Enforcement Act, or CALEA.[59] Under CALEA, providers are obligated to configure their networks to be able quickly to assist law enforcement monitoring. 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 but also to stave off future regulation.

Finally, many providers view new forms of network monitoring as a way to comply with Sarbanes Oxley, Graham Leach Bliley, HIPAA, and recent e-discovery changes to the Federal Rules of Civil Procedure. Vendors of monitoring products bolster these views by touting their DPI products as legal compliance tools.[60]

3. Signs of Change

As a result of advances in monitoring technology and pressures on ISPs to use new technologies to raise revenue and assist third parties, ISPs 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. This has happened at a breathtaking pace and suggests an undeniable trend.

a) 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.[61] Although BitTorrent users had long suspected that Internet Service Providers (ISPs) had been slowing down particular types of Internet traffic, Comcast's techniques seemed more aggressive and harder to evade.[62]

---

[58] Anne Broache, *RIAA: No Need to Force ISPs by Law to Monitor Piracy*, CNET, 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).

[59] Pub. L. No. 103-414, 108 Stat. 4279.

[60] Crosstec Security LLC, Product Flyer for ActiveWorx Security Center, http://www.crosstecsecurity.com/Default.aspx?tabid=53 (follow "Product Flyer" hyperlink) (last visited July 17, 2008) ("ASC includes over 200 reports for Sarbanes-Oxley, HIPAA, PCI, GLBA and more.").

[61] Blog post of Ernesto to TorrentFreak blog, Comcast Throttles BitTorrent Traffic, Seeding Impossible, August 17, 2007, http://torrentfreak.com/comcast-throttles-bittorrent-traffic-seeding-impossible/ (first public posting related to controversy).

[62] *Id.*

Eventually, the techniques were confirmed by the press[63] and activists[64] and the Federal Communications Commission (FCC) opened an investigation.[65] Throughout the ensuing firestorm, Comcast has repeatedly defended its actions as necessary steps to manage its network.[66]

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.[67] After reports of this behavior emerged, the Federal Communications Commission launched an investigation[68] and held two hearings.[69]

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.[70] 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.[71] Specifically, Comcast now plans to manage traffic based on bandwidth usage rather than application choice.[72]

On August 1, 2008, the FCC, in an unprecedented and landmark ruling, concluded that Comcast had "unduly interfered with Internet users'

---

[63] Peter Svensson, *Comcast Blocks Some Internet Traffic*, ASSOC. PRESS, Oct. 19, 2007 (Oct. 19, 2007), *available at* http://www.msnbc.msn.com/id/21376597/.

[64] Seth Schoen, *EFF Tests Agree with AP: Comcast is Forging Packets to Interfere with User Traffic*, ELEC. FRONTIER FOUND. DEEPLINKS blog, Oct. 19, 2007, http://www.eff.org/deeplinks/2007/10/eff-tests-agree-ap-comcast-forging-packets-to-interfere.

[65] *F.C.C. to Look at Complaints Comcast Interferes with Net*, ASSOC. PRESS, Jan. 9, 2008, *available at* http://www.nytimes.com/2008/01/09/business/media/09fcc.html.

[66] *E.g.*, Letter from Kathryn A. Zachem, Vice President, Regulatory Affairs, Comcast Corp. to FCC, July 10, 2008, *available at* 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.").

[67] Blog post of Ernesto to TorrentFreak, Comcast Wrongfully Denies Interfereing with BitTorrent, August 17, 2007, http://torrentfreak.com/comcast-wrongfully-denies-interfering-with-bittorrent/.

[68] *F.C.C. to Look at Complaints Comcast Interferes with Net*, ASSOC. PRESS, Jan. 9, 2008, available at http://www.nytimes.com/2008/01/09/business/media/09fcc.html.

[69] Steven Labaton, *F.C.C. Weighing Limits on Slowing Web Traffic*, N.Y. TIMES, Feb. 26, 2008, http://www.nytimes.com/2008/02/26/technology/26fcc.html; Ryan Kim, *FCC Hears Net Neutrality Arguments at Stanford*, S.F. CHRON., Apr. 18, 2008, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/04/17/BUM3107KI0.DTL.

[70] Comcast Press Release, Comcast and Bittorrent Form Collaboration to Address Network Management, Network Architecture and Content Distribution, March 27, 2008, *available at* http://www.comcast.com/About/PressRelease/PressReleaseDetail.ashx?PRID=740.

[71] *Id.*

[72] Vishesh Kumar, *Comcast, Bittorrent to Work Together on Network Traffic,* WALL STREET J., March 27, 2008 (quoting Comcast C.T.O. Tony Warner).

rights" and ordered the company to end its discriminatory practices, disclose more details about its practices, and disclose details about its replacement practices.[73] Comcast is likely to appeal the ruling.

b) AT&T's Plans for Network Filtering

A similar public firestorm has arisen over statements made by executives of AT&T. Last year, reports emerged that AT&T was in talks with movie studios and record producers to develop new monitoring and blocking technologies.[74] In January 2008, during a panel discussion on digital piracy when asked about the prospect of ISPs using "digital fingerprint techniques on the network level," an AT&T 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 . . . ."[75] Later that month, AT&T CEO Randall Stevenson confirmed that the company was evaluating whether to undertake this kind of monitoring.[76]

c) Phorm

A company called Phorm has been heavily scrutinized for its plan for a new method of targeting Internet marketing.[77] 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. By reconfiguring the ISPs' servers, Phorm will be able to access, analyze, and categorize websites users have visited into separate advertising channels.[78] If a user visits many travel-related websites she will begin to see more travel-related ads at Phorm-affiliated websites.[79] 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."[80]

Because these ads will be targeted to behavior, consumers will be more likely to click on them, justifying higher advertising rates and earning more money for Phorm, the ISP, and the website hosting the ad. The

---

[73] FCC Press Release, Commission Orders Comcast to End Discriminatory Network Management Practices, August 1, 2008, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-284286A1.pdf.

[74] Peter Burrows, *AT&T to Get Tough on Privacy*, BUSINESS WEEK, Nov. 7, 2007, http://www.businessweek.com/technology/content/nov2007/tc2007116_145984.htm (reporting that AT&T, NBC, and Disney had invested $10 Million in a company called Vobile, which develops a content recognition system).

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

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

[77] Louise Story, *A Company Promises the Deepest Data Mining Yet*, N.Y. TIMES, March 20, 2008.

[78] Richard Clayton, The Phorm "Webwise" System, http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf (Revised ed. May 18, 2008).

[79] *Id.*

[80] *Id.*

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.[81]

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,[82] 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 . . . ."[83]

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 TalkTalk as your Internet provider." [84] 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.[85]

d) 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.[86] Charter's Senior Vice President sent a letter to customers informing them of the plan and giving them instructions on how to opt out.[87]

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.[88] Congressmen Edward Markey and Joe Barton wrote a letter to Charter's CEO arguing that the plan might violate federal law and

---

[81] Charles Arthur, *TalkTalk to Make Phorm Use Opt-In, Not Opt-Out*, THE GUARDIAN, March 10, 2008, 4:37 PM, http://blogs.guardian.co.uk/technology/2008/03/10/talktalk_to_make_phorm_use_optin_not_optout.html. *See infra* Part I.B.3.c (discussing Phorm).

[82] Information Commissioner's Office (ICO), Who We Are, http://www.ico.gov.uk/about_us/who_we_are.aspx (visited June 25, 2008).

[83] ICO, Phorm—Webwise and Open Internet Exchange, http://www.ico.gov.uk/about_us/news_and_views/current_topics/phorm_webwise_and_oie.aspx (April 18, 2008).

[84] 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%27+spyware+tie-up/article.do.

[85] *Users Offered Ad Tracking Choice*, BBC NEWS, March 11, 2008, http://news.bbc.co.uk/2/hi/technology/7289481.stm.

[86] 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 78 at ¶ 19, while NebuAd injects code into a user's web browsing stream. Robert M. Topolski, NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking, http://www.freepress.net/files/NebuAd_Report.pdf (2008).

[87] Letter from Joe Stackhouse, Senior Vice President, Customer Operations, Charter Communications, May 14, 2008, *available at* http://graphics8.nytimes.com/packages/pdf/technology/20080514_charter_letter.pdf.

[88] Robert M. Topolski, NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking, http://www.freepress.net/files/NebuAd_Report.pdf (2008).

urging the company not to act until it had consulted with Congress.[89] The Senate Subcommittee on Interstate Commerce, Trade, and Tourism held a hearing about interactive advertising prompted by the controversy.[90] Connecticut's Attorney General also released a letter urging Charter not to implement the program.[91] In the face of this criticism, about a month after announcing the plan, Charter abandoned it.[92] In the meantime, NebuAd has partnered with other, smaller ISPs, some of which have already implemented the program.[93]

4. Is Any of this Unethical?

If falling technological barriers and new market pressures have pushed these providers to invade user privacy in new ways, what about Lessig's third regulator, norms or ethics? Legal scholars have long examined how society develops ethics and norms to foster private ordering without law.[94] Ethics have played only a very minor role in the disputes detailed here, because network monitoring is a norm-light space where ethical rules are rarely articulated and poorly understood. Providers have taken advantage of this vagueness to try to use public relations to redefine ethical standards in their favor.

All four of the cases cited above involved techniques that some experts have stated publicly breach ethics, likening some of the tactics even to criminal behavior. Comcast's use of TCP reset packets has drawn a bevy of criticism.[95] Although forged TCP reset packets do not clearly violate Internet protocols,[96] other ISPs tend not to use them for this type of

---

[89] Letter to Mr. Neil Smit, President and CEO of Charter Communications from Reps. Edward J. Markey and Joe Barton, May 16, 2008, *available at* http://markey.house.gov/docs/telecomm/letter_charter_comm_privacy.pdf.

[90] 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.

[91] Jim Salter, *Charter Drops Web Tracking Plans*, ASSOC. PRESS, June 24, 2008, available at http://news.yahoo.com/s/ap/20080625/ap_on_hi_te/charter_web_tracking.

[92] *See* Saul Hansell, *Charter Suspends Plan to Sell Customer Data to Advertisers*, N.Y. TIMES BITS BLOG, June 24, 2008, 5:02 PM, http://bits.blogs.nytimes.com/2008/06/24/charter-suspends-plan-to-sell-customer-data-to-advertisers/.

[93] Stephanie Clifford, *Web Privacy on the Radar in Congress*, N.Y. TIMES, Aug. 10, 2008.

[94] ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991).

[95] Statement of David P. Reed, Adjunct Professor, MIT, to the FCC, Feb. 25, 2008 ("Neither Deep Packet Inspection nor RST Injection are acceptable behavior by Autonomous Systems in the Internet, for a simple reason: they each violate the expectation that the contents of the envelopes are untouched inside and between Autonomous Systems.").

[96] In the original version of the TCP protocol, embodied in a document called RFC 793 adopted in 1981, the IETF defined TCP reset packets and sketched some norms for their use, "As a general rule, reset (RST) must be sent whenever a segment arrives which apparently is not intended for the current connection. A reset must not be sent if it is not clear that this is the case." RFC 793: Transmission Control Protocol, DARPA Internet Program Protocol Specification at 35 (Jon Postel, ed. 1981). Much later, the IETF adopted a "Best Current Practice" written by Dr. Sally Floyd entitled "Inappropriate TCP Resets Considered Harmful." S. Floyd, RFC 3360: Inappropriate TCP Resets Considered Harmful (Best Current Practice) (2002). In this document, Dr. Floyd points to RFC 793 and other IETF documents

congestion control. Some experts have criticized the practice as illicit hacking.[97] It does not help Comcast's public relations efforts that China uses the very same technique to prevent its citizens from visiting banned sites.[98]

Likewise, an MSNBC blogger has called AT&T's filtering plans "unethical, impractical, insane, and given the CEO's explanation, probably more than a little dishonest."[99]

Similarly, NebuAd has been accused of engaging in unethical behavior. According to a report by Robert Topolski, an expert hired by net neutrality crusaders Free Press and Public Knowledge, NebuAd engages in "browser hijacking, cross-site scripting and man-in-the-middle attacks," techniques which "violate several fundamental expectations of Internet privacy, security and standards-based interoperability."[100] As one example, Topolski points to how NebuAd "injects" extra code into the webpage returned by Google, forcing the customer's web browser to download code from a third-party unrelated to Google.[101]

Phorm also takes advantage of techniques once the province of malicious hackers. In order to characterize every website a user visits, Phorm sends user computers http redirects—electronic notices designed to inform the user's browser that a website has moved—redirecting the user to a Phorm-run website instead. It does this to fool the user's computer into accepting cookies that appear to come from Google, say, but actually come from Phorm. Richard Clayton, a researcher who has been critical of Phorm, calls this "forging cookies" and also "clearly illegal" under British law.[102]

Providers and vendors have counteracted claims of unethical behavior in various ways. They have simply protested that they have acted ethically. For example, in a filing to the FCC, Comcast took issue with characterizing its use of RST packets as "forgery."[103] It never explained, however, why the technique is anything but forgery, under either the technical or plain meaning of the word.

---

to argue against firewalls who use TCP reset packets in some forms of congestion control. *Id.* at 1.

[97] Peter Eckersley, Fred Von Lohmann, and Seth Schoen, Packet Forgery by ISP: A Report on the Comcast Affair, Nov. 28, 2007, at 5 ("Comcast is essentially deploying against their own customers techniques more typically used by malicious hackers."), *available at* http://www.eff.org/files/eff_comcast_report2.pdf.

[98] Richard Clayton, Steven J. Murdoch & Robert N.M. Watson, *Ignoring the Great Firewall of China*, 3 I/S: A J. OF L. & POLICY FOR THE INTERNET SOC'Y 271, 276-80.

[99] Helen A.S. Popkin, *AT&T's Proposed Filtering Policy is Bad News*, MSNBC.COM, Jan. 25, 2008, http://www.msnbc.msn.com/id/22829568/.

[100] Robert M. Topolski, NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking, http://www.freepress.net/files/NebuAd_Report.pdf (2008).

[101] *Id.* at 6.

[102] Richard Clayton, Slides from talk presented to 80/20 Thinking Town Hall meeting, at slide no. 10, http://www.lightbluetouchpaper.org/2008/04/22/stealing-phorm-cookies/ (click "my slides" link in first paragraph).

[103] Comments of Comcast Corp. Before the F.C.C., Feb. 12, 2008, available at http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6519840991 (calling the use of the word "forged," "inflammatory hyperbole, not fact.").

Providers have also found expert defenders to speak on their behalf. Phorm, for example, hired noted privacy specialist Simon Davies to conduct a privacy audit of its system. Mr. Davies concluded that his company was "impressed with the effort that had been put into minimising the collection of personal information."[104] In fact, in its interim privacy impact assessment, Mr. Davies' consulting firm lamented that Phorm's service "will be perceived as invasive."[105]

In network monitoring, the ethics were never well-delineated to begin.[106] There are no codified rules of accepted practice to which new systems administrators can turn to learn to distinguish black from white; everything is somewhat gray.[107] Rules are passed down from elder to acolyte, and rules vary from institution to institution if not within the same institution.[108] For many, the only rule they ever learn is, "it's my network, and I can do what I want with it." All of this adds up to a fragile ethical framework that is easy to shift and alter.

5. Forecast

I predict that ISPs, faced with changes in technology, extraordinary pressures to innovate, and murky ethical rules, will continue aggressively to expand network monitoring. The AT&T, Comcast, Charter, NebuAd and Phorm examples will prove to be not 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.

As proof of this trend, consider the rise of the "deep-packet inspection" (DPI) industry.[109] These companies sell hardware and software tools which consume packets voraciously, like packet sniffers, but monitor at all times, whether or not the ISP has specific cause. 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.[110] Sales of DPI

---

[104] Darren Waters, *Ad System 'will protect privacy'*, BBC NEWS, March 6, 2008, http://news.bbc.co.uk/1/hi/technology/7280791.stm.

[105] 80/20 Thinking Ltd., First Stage (Interim) Privacy Impact Assessment, Feb. 10, 2008, http://privacy.phorm.com/Phorm_PIA_interim.pdf.

[106] Abe Singer, *Conference Password Sniffing*, ;LOGIN: at 7 (Aug. 2005) (describing how network monitoring ethics shift over time); Marc Allman and & Vern Paxson, *Issues and Etiquette Concerning Use of Shared Measurement Data*, PROCEEDINGS OF THE 2007 INTERNET MEASUREMENT CONFERENCE (same).

[107] *See* Singer, *supra* note 106.

[108] *See* Allman & Paxson, *supra* note 106, at 135 ("[W]e have been struck by the range of attitudes and assumptions present in the community . . . .").

[109] *Cf.* Wu, *supra* note 20, at 163-64 (predicting future restrictions providers might impose on network neutrality by surveying "the marketing efforts of equipment vendors who target the cable and DSL market").

[110] Light Reading Industry, *supra* note 51.

products in 2007 reached $400 million and are expected to rise to one billion dollars in 2010.[111]

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."[112] Another vendor, Endace, uses the motto, "Power to see all."[113]

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

C. The Threat to Privacy

1. Conceptualizing Privacy

As Professor Dan Solove puts it, privacy "is a concept in disarray."[114] 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.[115]

As a way out of this morass, Professor Solove recommends a four-pronged approach for setting out theories of privacy,[116] most of which I adopt here. Solove is a self-avowed pragmatist striving to provide solutions to real-world problems.[117] This is my goal, as well. First, he eschews searches for "rigid conceptual boundaries and common denominators" in favor of a Wittgensteinian "family resemblances" approach.[118] 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 distinct yet related things."[119]

His second recommendation is that privacy should be discussed neither too specifically nor too generally.[120] Solove says that we should simultaneously "resolve privacy issues by looking to the specific context,"[121] while at the same time use "a general framework to identify privacy harms or problems and to understand why they are problematic."[122]

---

[111] Kyle, Deep Packet Inspection: Vendors Tap Into New Markets, dPacket.org blog, Nov. 28, 2007, https://www.dpacket.org/articles/deep-packet-inspection-vendors-tap-new-markets (summarizing Light Reading report).
[112] Solera Networks, Top 10 Reasons for Deep Packet Capture and Stream-to-Storage, http://www.soleranetworks.com/solutions/top-ten.php (last visited July 11, 2008).
[113] Endace home page, http://www.endace.com/ (last visited July 11, 2008).
[114] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008) [*hereinafter* SOLOVE, UNDERSTANDING PRIVACY].
[115] *Id.*
[116] *Id.* at 401-41.
[117] *Id.* at 47-49.
[118] *Id.* at 42-44.
[119] *Id.* at 40.
[120] *Id.* at 46-49.
[121] *Id.* at 48.
[122] *Id.* at 49.

Third, Solove embraces a dynamic view of privacy, because notions of privacy change over time and place. [123] Finally, he advocates a focus on problems instead of preferences, expectations, or types of information as his organizing principle.[124]

Applying Solove's framework, this Article focuses at first narrowly on network management practices as a threat to privacy. Accepting Solove's exhortation to generalize, the Article works from the bottom up, applying the lessons from this context into a broader theory of communications privacy.

2. Information Exposure

Is there reason to regulate ISP monitoring now, or should regulators wait to see if some combination of the market, norms, ethics, and self-regulation will protect user privacy? To answer these questions, we need to understand the potential harms—what Solove calls problems—of ISP monitoring. Harms from privacy can be assessed 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.[125] 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.

I propose a three-step process for assessing the likelihood of future significant harm to privacy. First, and most importantly, how much private information is at risk? If the answer is, "not much," 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 of information revealed by complete monitoring.

When great amounts of private information are 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, 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.

In this case, these three steps lead to the conclusion that the threat of serious invasions of privacy by ISPs is significant, and in need of oversight.

---

[123] *Id.* at 50-51.
[124] *Id.* at 74-76.
[125] I have critiqued the harmful effects of speculation and science fiction in an earlier work. Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1330 (2008).

a) ISPs Compared to Other Online Entities

Let us start with the first prong: how much personal information flows through an ISP's wires and is stored on it computers? In modern connected life, almost no other entity poses a greater threat to privacy than the ISP. ISPs pose a much greater threat to privacy than other online entities and they even pose a greater threat than offline institutions as well, including doctors, psychiatrists, and lawyers.

Because the ISP is the gateway—the first hop—to the Internet, almost any communication sent to anybody online is accessible to the ISP as well. Compare the amount of information accessible to an ISP with the amount of information accessible to Google, a company that receives a lot of attention for its privacy practices, despite a relatively clean record of past performance.[126]

Today, Google has archived more information about an individual'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.[127] These search queries can be sniffed by ISPs, and both Phorm and NebuAd specifically ferret out Google search queries from user packets.[128]

The same is true for most 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, browses blogs on Google Reader, edits a word processing document in Google Docs, or views a video in Google-owned YouTube, he must first route those messages, requests, and behavior through his ISP.[129]

Thus, the ISP can access all of the information available to Google.[130] Anything that can be said about Google's threat to privacy can also be said about an ISP. But this is the important part: this is only a small slice of the ISP's information pie; the ISP can also access communications sent to and from Yahoo!, Microsoft, AOL, Myspace, Facebook, eBay,

---

[126] 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 Bits*, 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/.

[127] *See* Grimmelmann, *supra* note 2, at 18.

[128] Clayton, *supra* note 78, at ¶¶ 46, 56-57 (describing Phorm's use of search terms); Topolski, *supra* note 88, at 6 (describing NebuAd's interception of Google data).

[129] *Cf.* Humphrey Cheng, *Point and Click Gmail Hacking at Black Hat*, TG DAILY, August 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).

[130] 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. Walaika Haskins, *Google Will Forget You Asked*, TECHNEWSWORLD, March 15, 2007, http://www.technewsworld.com/story/56321.html. So, it might take a year and a half from the time ISPs flip the switch saving everything until they surpass Google's collection.

Wikipedia, Amazon, and Craigslist, as well as the millions of websites unaffiliated with 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.[131] 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) What ISPs Cannot See: Encrypted Contents and Use of Another ISP

There are two important exceptions to the all-seeing eye of ISPs: they are blind to the communications of users using another ISP and to the contents of encrypted communications. ISPs cannot see the communications of their users when they are using a different provider. Many people surf the web at home as well as at work, and increasingly, on their mobile phones. Thus, unlike Google, which can associate behavior at each of these three connections to the same unique login ID, the residential ISP sees only part of the picture. Still, this is likely to be a broad part. Given the amount of time people spend online, if a typical user splits his browsing into three-equal parts, each part will still contain a significant amount of personal information.[132]

Second, an ISP cannot decipher its user's encrypted communications. In particular, when a website uses the SSL protocol (signified by the little lock icon in the user's browser) it wraps all of the content within a tunnel of encryption. If Gmail is viewed through SSL, an ISP cannot read the users' e-mail messages.[133]

The encryption exception does not swallow the rule for at least two reasons. First, most websites do not use SSL because it is difficult and expensive to implement[134] and slows the user's browsing experience.[135] Gmail, for example, disables SSL by default. Second, even though ISPs

---

[131] 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 dozens (at least) of different services. JOHN BATELLE, THE SEARCH (2005).

[132] Nielsen reports that the average American Internet user spends 26 hours online per month. The Nielsen Co., Nielsen's Three Screen Report (May 2008), *available at* http://www.nielsen.com/pdf/3_Screen_Report_May08_FINAL.pdf.

[133] 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).

[134] 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: SOLUTIONS AND EXAMPLES FOR BUILDING AND ADMINISTERING YOUR WEB SITE 206 (2006) ("SSL certificates are not cheap, and they must be renewed every year or two.").

[135] Sogohian, *supra* note 133 (speculating that Gmail defaults to no SSL for performance reasons, saying "I'm guessing. 10 million users all requiring an SSL handshake is expensive in processing power.").

cannot read encrypted messages, they can use so-called "traffic analysis" techniques to reveal some personal information from encrypted data streams.[136] Italian researchers have demonstrated a method they call a "tunnel hunter" which can be "trained" to distinguish ordinary encrypted ssh from other protocols masquerading as ssh.[137] Some have alleged that Comcast has been able to detect and throttle encrypted BitTorrent packets masquerading as something else.[138]

c) 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 for well-connected people, nearly everything told to these three types of people is now revealed 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, giving the ISP access to this information too.[139] 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 IM; 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,[140] records held by financial institutions,[141] educational records,[142] and video viewing records[143] are all restricted from certain types of disclosure, use, or

[136] By raising the specter of a sophisticated ISP attack, this might be an example of the Myth of the Superuser I have condemned elsewhere. Ohm, *supra* note 125. Then again, ISPs have the motivation, tools, know-how, and resources to conduct sophisticated monitoring. *Infra*. This fact counteracts, at least somewhat, the usually completely unsupported use of the Myth.

[137] Maurizio Dusi, Manuel Crotti, et al., *Detection of Encrypted Tunnels Across Network Boundaries*, 2008 IEEE INT'L CONF. ON COMM. PROC. 1738.

[138] Post of Ernesto to TorrentFreak blog entitled BitTorrent Developers Introduce Comcast Busting Encryption, Feb. 15, 2008, http://torrentfreak.com/bittorrent-devs-introduce-comcast-busting-encryption-080215/.

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

[140] Driver's Privacy Protection Act of 1994, Pub. L. No., 103-322, 108 Stat. 2099 (codified at 18 U.S.C. §§ 2721-25).

[141] Right to Financial Privacy Act, Pub. L. No. 95-630, 92 Stat. 3641 (codified at 12 U.S.C. §§ 3401-3420 (2000).

[142] Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 44 (codified at 20 U.S.C. § 1232g).

[143] Video Privacy Protection Act, Pub. L. No. 100-618, 102 Stat. 3195, (codified at 18 U.S.C. § § 2710-11).

collection under federal law. What is contained in these databases pales in comparison to what an ISP can access.

d) Potential Harms

Solove's fourth prong focuses on the problems of privacy. He prefers this to other approaches that have focused on things like personal preferences or expectations of privacy. How are people harmed, inconvenienced, or otherwise troubled when ISPs monitor?

Imagine that an ISP conducts complete monitoring on one user for one month. The data it collects contains information about everything the user does on the Internet for the month. The complete content of every web page visited is stored. Every e-mail message sent or received is logged. The collection contains every instant message, video download, tweet, facebook update, file transfer, VoIP conversation, and more.

The potential inconvenience, embarrassment, hardship, or pain that can result because the ISP collects this trove of data 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 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.[144] An ISP can know 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 number or bank account information 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."[145] 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 that Professor Solove has written about at least take some effort and expense to assemble.[146] Companies wishing to compile them need to buy and mine the data, requiring money, technology, and human capital. An ISP needs 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 is much broader.

---

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

[145] Olmstead v. United States, 277 U.S. 438, 475-76 (1928) (Brandeis, J., dissenting).

[146] SOLOVE, DIGITAL PERSON, *supra* note 3.

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 which had intentionally declined to log data about visitors for privacy's sake to turn on logging to reveal potential copyright infringers;[149] and the Department of Justice, in a civil case, subpoenaed search engine query archives from Yahoo!, Microsoft, and Google.[150]

A lot of recent privacy scholarship has tried to provide theoretical accounts of the potential harms of information privacy breaches. 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,"[151] 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. Consider a few.

Professor Julie Cohen describes the benefits of psychological repose, which can be undermined from surveillance.[152] 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."[153]

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,

---

[147] Saul Hansell, *One Subpoena is All it Takes to Reveal Your Online Life*, N.Y. TIMES BITS BLOG, July 7, 2008 ("[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.

[149] Columbia v. Bunnell, 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, May 29, 2007 , available at 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 (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. CHRONICLE, March 15, 2006.

[151] Reno v. ACLU, 521 U.S. 844, 852 (1997).

[152] Julie Cohen, *Examined Lives: Information Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425 (2000).

[153] *Id.*

understanding that the New York Times tracks which articles we read on their site but has no way of knowing what we do when we visit the Washington Post.[154] These expectations are violated 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."[155] We will lose, in her terms, "the expression of eccentric individuality."[156]

Other scholars discuss the harms of pervasive electronic surveillance. Paul Schwartz argues that "perfected surveillance of naked thought's digital expression short-circuits the individual's own process of decisionmaking."[157] Jerry Kang notes how surveillance can lead to self-censorship.[158]

The question of harm has often bedeviled privacy scholars.[159] 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.

3. ISPs have a Track Record of Respecting Privacy

Because ISPs possess a vast—uniquely vast—potential data reach the analysis must continue. The second step is to see if ISPs have historically abused their potential power. Despite the potential harms an ISP could cause, there are few examples of past breaches. No reported cases have ever discussed the liability of an ISP for unlawfully running packet sniffers, except for lawsuits against providers for supporting government monitoring.[160] Telephone companies and their employees have been sued and criminally charged more often, 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.[161] Some of these cases will be discussed in greater depth in

[154] 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.

[155] Cohen, *supra* note 152 at 1426.

[156] *Id.*

[157] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1656 (1999).

[158] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1260 (1998).

[159] Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745.768-72 (2008).

[160] EFF, Hepting v. AT&T, http://www.eff.org/cases/hepting (last visited August 1, 2008) (collecting materials relating to lawsuit against AT&T for assisting NSA monitoring program).

[161] U.S. v. Pervaz, 118 F.3d 1 (1st Cir. 1997); U.S. v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993); U.S. v. McLaren, 957 F. Supp. 215 (M.D. Fla. 1997); Sistok v. N.W. Tel. Sys. Inc., 189 Mont. 82 (1980).

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.[162]

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.[163]

4. Constraints—and Signs of Evaporation

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

Many recent scholars have focused on the role of code as a regulator of online conduct.[164] To adapt an argument from Professor Harry Surden, the limits of ISP monitoring technology have guaranteed users a *structural constraint right* in privacy.[165] But this constraint right has been recently breached. Surden argues that as latent constraint privacy rights evaporate, policymakers should consider reinstituting those rights by enacting laws.[166]

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. 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 have arisen, we need to ask if another regulatory force—law—must fill the gap.

5. Thought Experiment: What if Microsoft Started Monitoring?

Falling constraints are the critical part of this argument. This Article is not arguing that ISPs must be regulated only because they have the potential to access a vast amount of sensitive information. A few companies have access to as much or more information about users than ISPs, yet they

---

[162] *See, e.g.*, Pervaz, 118 F.3d at 6; McLaren, 957 F. Supp. at 219-20.

[163] *E.g.* Joseph Pereira, *How Credit-Card Data Went Out Wireless Door*, WALL ST. J., May 4, 2007 (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.); Nakashima, *supra* note 211 (describing release of AOL search queries).

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

[165] Harry Surden, *Structural Rights in Privacy*, 60 S.M.U.L. REV. 1605 (2007).

[166] *Id.* at 1619.

need not be regulated today. Consider Microsoft. As the developer of Operating Systems (OS) used by more than 90% of worldwide users,[167] 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 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 revealed no plans indicating the company's moves to monetize user information.[168] 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 saying in 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.

6. Conclusion: We Must Regulate ISP 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 restrict ISP monitoring. Although much work—descriptive, predictive, and normative—has already been done, the hardest analyses lay ahead. Thus far, this Article has analyzed only the worst case—the risks from complete monitoring. Because ISPs are likely to want to do something approaching complete monitoring, possibly through deep-packet inspection, a law should ban the most invasive forms of monitoring. The more difficult and important question is how much other conduct—conduct

---

[167] Onestat.com Press Release, Microsoft's Windows Vista Global Usage Share is 13.24 Percent on the Web According to OneStat.com, April 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."); .

[168] 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, July 25, 2008 (reporting that Microsoft "was working diligently on narrowing the [search query] advertising gap [with Google]").

that invades less privacy than complete monitoring—should policymakers regulate?

II. TOWARDS A NEW THEORY OF COMMUNICATIONS PRIVACY

In Part IV, this Article will demonstrate how the federal and state wiretapping laws 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. Before analyzing those laws, let us start with a blank slate and ask, what 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 developing a normative theory of communications privacy. Then, in Part III, it applies this new theory to propose prescriptions for an ideal ISP monitoring regulation.

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"[169] of the communication—more vigorously than it protects the non-content "dialing, routing, addressing, and signaling information."[170]

We could unthinkingly apply the envelope analogy to the Internet, declaring that a packet too is like a closed letter in the mail, with non-content headers stamped outside the envelope and the content sealed within.[171] This analogy would be flawed; for one thing, there is more than one envelope. Think of a packet like a Russian nesting doll. Packets are built up in successive layers of information each one wrapped around all of the "inner" layers that have come before through a process called encapsulation.[172] 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, underprotective, and gives rise to

---

[169] 18 U.S.C. § 2510(4), (8).

[170] 18 U.S.C. § 3127(3), (4). These laws apply to network monitoring as well. For much more on these laws, see Part IV.A.

[171] Statement of Dr. David P. Reed, Adjunct Professor, Massachusetts Institute of Technology, to the Subcommittee on Telecommunications and the Internet, Committee on Energy and Commerce, U.S. House of Reps., July 17, 2008 ("I avoid 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.").

[172] DAVID G. MESSERSCHMITT, UNDERSTANDING NETWORKED APPLICATIONS: A FIRST COURSE 519-20 (1999).

question begging and difficult line drawing.[173] 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.[174] 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 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.[175] 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.[176] At any given layer in the Russian-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.[177] If this view were

---

[173] *See* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 114, at 13 (criticizing earlier conceptions of privacy as being too narrow, too broad, or sometimes both).

[174] Solove, *Reconstructing*, *supra* note 144, at 1288 ("Envelope information can be quite sensitive; content information can be quite innocuous.").

[175] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 114, at 116-21 (discussing the harms that can result from data aggregation).

[176] 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 (2003). He gives the specific example of comparing the privacy of online communications to physical mail. *Id.* at 365-68.

[177] In fact, there are layers "above" IP, the datalink and physical layers. From their vantage point, IP information may seem like content. Comment of user "eck" to Volokh Conspiracy Blog dated June 18, 2008, 8:43pm, http://volokh.com/posts/1213821576.shtml#388008 ("[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

adopted, then ISPs would have no business accessing the To: and From: lines of email messages.

B. Contextual Integrity

Once we abandon the envelope analogy, we need another normative frame that is more sensitive to the problems of context and non-universality. Professor Helen Nissenbaum has proposed a benchmark for measuring privacy called "contextual integrity."[178] She favors it over what she calls "traditional" factors, which raise difficult line-drawing problems and arrive at the wrong conclusions when compared to what we really value when we call something private, at least for hard problems.[179]

Contextual integrity is about respecting societal norms of privacy that people hold about their information.[180] These are not global, universal norms such as "things you do in public can be monitored by other people," but instead these are norms associated with narrowly-defined contexts.[181] This is a fine-tuned theory about how our attitudes about privacy expand and contract as we move from context to context in our daily lives.[182] Contextual integrity uses these attitudes as a starting point for regulation.

There are some problems with the approach—most importantly a status quo bias which Nissenbaum acknowledges and I will critique later—but I find much to admire in contextual integrity and follow its basic prescriptions. The approach is quite compatible with Professor Solove's four-pronged approach to conceptualizing privacy, and in fact, he cites contextual integrity in developing his structure.[183]

To begin, we must choose a context. Nissenbaum says little about how to select a context of appropriate size and scale, except to say that sweeping contexts like education, politics, and the marketplace are bites too big to chew. The context of this Article—user monitoring by ISPs—seems similar, or perhaps a bit narrower, in scale to some of the examples she discusses—mail-order merchants, doctor-patient confidentiality, and the job application process, to name three.[184] Like these three examples, ISP monitoring seems appropriately discrete and uniform. Broadening the context—for example to include websites operators like Google or digital dossier compilers like ChoicePoint would seem to introduce too much norm variability, as will be discussed later.[185]

What are the "informational norms" of ISP monitoring? Nissenbaum proposes two general categories: "appropriateness norms,"

---

informed commentators would still say that source/destination IP addresses are addressing info, layer encapsulation notwithstanding.").

[178] Helen Nissenbaum, *Technology, Values, and the Justice System*, 79 WASH. L. REV. 119 (2004).

[179] *Id.* at 125.

[180] *Id.* at 138.

[181] *Id.* at 137.

[182] *Id.* at 138.

[183] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 114, at 47-48.

[184] Nissenbaum, *supra* note 178, at 142-43.

[185] *See infra* Part III.B.2.b.

which "dictate what information about persons is appropriate, or fitting, to reveal in a particular context," and "distribution norms" which "govern [the] movement or transfer of information from one party to another."[186]

"Appropriateness" seems question begging and thus unhelpful in this context. Do people find ISP monitoring appropriate or inappropriate? Now that is the question, is it not? Nissenbaum's examples of appropriateness norms arise in contexts—friendships, doctor-patient, the classroom, the courtroom—that are ancient, particularly compared to ISP monitoring.[187] With time, a clearer understanding of what is appropriate may evolve online, but without the ability to draw on ancient signals, the appropriateness norm is circular, in the same manner as the objective prong of the Fourth Amendment's reasonable expectation of privacy test,[188] and thus of little use in the ISP monitoring context.

Nissenbaum's other norm, distribution, is more resistant to question-begging. She gives as examples of distribution norms, expectations of free choice, discretion and confidentiality. For example, we expect friends not to try to compel us to reveal private information, and when we do choose to reveal secrets, our friends must treat the information confidentially.[189]

In addition to these examples, Nissenbaum offers three other distribution norms which are central to the ISP monitoring question: "need, entitlement, and obligation."[190] As examples of these, she notes that doctors will not treat patients who refuse to reveal symptoms and mail-order companies will refuse to ship products to those who decline to disclose credit card numbers and shipping addresses.[191] In the ISP monitoring debate, arguments often come down to competing claims about need. What must an ISP be allowed to do in order to provide service and protect its network? The hard part will be distinguishing needs from wants from mere conveniences. In the next Part, this Article will discuss a theory for measuring provider need.

Two other candidate norms are raised repeatedly in the debates over ISP monitoring: consent and anonymization. We will take up all of these justifications in Part III.

C. A Call for More Searching, Skeptical Balancing

Privacy is not absolute; society balances it against other values, most often security.[192] Policymakers balance security and privacy when deciding whether to enact a privacy-enhancing regulation; judges weigh the

---

[186] Nissenbaum, *supra* note 178, at 138-40.
[187] *Id.* at 139.
[188] Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974).
[189] Nissenbaum, *supra* note 178, at 142.
[190] *Id.*
[191] *Id.*
[192] RICHARD POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY (2006).

values when deciding whether a practice like government data mining violates the Fourth Amendment.

Despite the centrality of balance in the process, it is rarely done well. In a recent essay, Dan Solove complains that "the scale is rigged so that security will win out nearly all of the time."[193] Solove's critique is accurate, but he misses his target, because he blames only judges and policymakers for balancing blunders. In fact, privacy activists and scholars are as bad at balancing as anybody and given their role as agents for reform, they probably deserve much more blame. In fact, although Solove should be duly lauded for casting a light on the problems with balance, even he makes critical balancing errors in the very same essay.

The problem is over-deference. We defer too much to the security side of the scale, in part because it is often bound up in government secrets and technological complexity. We also defer to claims of expertise from those arguing for security. Solove calls overdeference by judges "an abdication of their function."[194]

These judges have some good company, because some of the most interesting and important recent works about privacy fail to say anything interesting about opposing values like security. In Professor Julie Cohen's important early work on online privacy, she spends very little time on weighing interests offsetting privacy, concluding with little discussion at one point that "[t]he baseline presumption should be one of strong data privacy protection; exceptions should be carefully considered and narrowly circumscribed."[195]

Likewise, Paul Schwartz calls for what he call "constitutive privacy,"—the idea that privacy can "help form the society in which we live in and shape our individual identities" as an alternative to the "right of control."[196] Like Cohen, he concedes that constitutive privacy is not absolute, but he is vague about when it yields, describing "shifting, multidimensional data preserves that insulate personal data from different kinds of observations by different parties."[197]

Helen Nissenbaum, whose work sets the basic normative frame for this Article, spends four or five pages of her article on contextual integrity recapping earlier work on "fundamental values that may be served by" privacy.[198] On the other side of the scale, she devotes one sentence with a few citations to the "many reasons for favoring the collection, sharing, and widespread distribution of personal information."[199]

Instead of engaging the other half of the balance, to try to question their conclusions about opposing values thereby tipping the scales in favor of privacy, these scholars pile weight on the privacy side, trying to elevate

---

[193] Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 362 (2008).
[194] *Id.* at 349
[195] Cohen, *supra* note 152 at 1432.
[196] Paul Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 834 (2000).
[197] *Id.*
[198] Nissenbaum, *supra* note 178, at 147-151.
[199] *Id.* at 151.

the importance of privacy by developing a rights-based vision of privacy's importance for autonomy,[200] deliberation,[201] free speech,[202] even democracy.[203] Instead of a balancing scale, this work evokes the image of an arms race with privacy scholars stockpiling privacy's values, making evermore sophisticated arguments.

The problem is that all of this privacy stockpiling makes privacy seem more abstract, more diffuse, and less tied to practical experience and salient harm. These viewpoints, supported by many citations to moral philosophers, make privacy seem much more abstract and unmoored. This is not to say these arguments are flawed or contrived. On the contrary, they are elegantly stated and proved.

But because these arguments are abstract, they are much less likely to impact public policy. Lawmakers understand salient, individual harms. They legislate because someone dies, not because a philosopher tells them they should. Ann Bartow has lodged this criticism about Dan Solove's work in particular, stating that "the Solove taxonomy of privacy suffers from too much doctrine, and not enough dead bodies."[204] This critique should concern these pragmatist scholars. Solove, in particular, seeks to conceptualize privacy in a way that is useful to lawmakers.

I think that this approach springs from a deep frustration with past policy failures. Although policymakers and the general public always claim to value policy, they rarely block invasive practices. These scholars, disheartened by these failures, have attributed them to the public's *undervaluing* privacy.[205] They have it backwards: the public seems to be *overvaluing* security.

The better approach is to attack—rigorously and systematically—the arguments in favor of the values opposing privacy. There is a man-behind-the-curtain quality to many of the claims in defense of more information flow and less privacy. Solove understands this, urging "[j]udges and legislators [to] require the experts to persuasively justify the security measures being developed or used."[206] Despite this exhortation, Solove fails to follow his own advice. To demonstrate what greater scrutiny looks like, he critiques the security claims justifying subway bag searches and data mining, but he does so in a thoroughly inexpert manner.[207] Subway bag searches are "largely symbolic . . . [and] unlikely to catch or deter terrorists because they involve only a miniscule fraction of the millions of daily

---

[200] Cohen, *supra* note 152.
[201] Schwartz, *supra* note 196, at 834.
[202] Neil Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1145 (2005).
[203] Schwartz, *supra* note 157, at 1656.
[204] Ann Bartow, *A Feeling of Unease About Privacy Law*, 155 U. PENN. L. REV. PENNUMBRA 52, 52.
[205] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 114, at 89 ("The problem with framing privacy solely in individualistic terms is that privacy becomes undervalued.").
[206] Solove, *supra* note 193, at 349.
[207] *Id.* at 352-53.

passengers."[208] Data mining has "little proven effectiveness," he argues, based on some quick calculations premised on speculation about false positive rates. He cites no expert opinions or reports to support any of these arguments. His analysis rests only on basic logic, guesses about things like success rates, and quick calculations. Arguments like these are likely to be easily rebutted, and stand little chance of flipping public opinion.

The better approach is to engage arguments against privacy with rigor, expert analysis, and proven methodologies. Engaging the other side using their methods will often reveal the disconnect between the arguments made in the name of security or efficiency and what the evidence can support. I embrace and demonstrate this approach in Part III.

D. The Theory

Putting these pieces together, my theory guides regulators trying to decide when to regulate communications privacy. Regulators should abandon the envelope analogy, because it maps imperfectly onto what we think should be private and requires difficult line drawing. Instead, they should embrace contextual integrity, which is a search for the preexisting norms of privacy and scrutiny in the conflicted space.

Where my theory diverges most from Nissenbaum's and from the work of the New Privacy Scholars is in setting out what to do when norms are difficult to ascertain. First, my theory focuses primarily on traditionally defined claims of individual harm, eschewing suggestions to look to abstract claims of societal harm. It discounts societal harms first because they tend to be so abstractly drawn as to be difficult to articulate and second, because policymakers tend to ignore these harms.

Second, my theory mandates a searching, skeptical dissection of claims opposing privacy such as claims of security and necessity. It refuses to accept unsupported claims and unscientific speculation about the need to gather and redistribute information. Instead, it requires expert proof of not only the need but also a tight connection between need and the monitoring proposed.

III. REGULATING NETWORK MONITORING

According to my theory of communications privacy, we must skeptically scrutinize ISP claims justifying their new types of invasive monitoring. There are three different claims they tend to make, which are all claims of norms of distribution in Nissenbaum's parlance. First, ISPs often argue that they comply with society's norms whenever they anonymize or aggregate the data they collect enough to prevent associations between the data and the user. I conclude in Subpart A that this is a plausible norm 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. In order to assess these claims and provide a specific

[208] *Id.* at 352.

prescription, Subpart B takes a detailed, technical look at what ISPs do. Finally, ISPs claim they monitor with their users' consent. Consent is a problematic topic, and I propose a novel mode of analysis in Subpart C.

A. Anonymization and Aggregation are Usually Not Enough

Aggregation and anonymization 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. 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. 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 it—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.

Even online, there seems to be a sense—a norm of distribution if you will—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.[209] 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.[210] 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

---

[209] Google, Zeitgeist: Search Patterns, Trends, and Surprises, http://www.google.com/press/zeitgeist.html (last visited July 30, 2008).

[210] Google, Google Zeitgeist 2007, Showbiz, http://www.google.com/intl/en/press/zeitgeist2007/showbiz.html (last visited July 30, 2008).

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.[211] 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.[212] Others had searched for child pornography or advice on how to kill a spouse.[213] 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.[214]

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.[215] I will focus on Phorm because its mechanisms are better documented.[216] Phorm is correct that the steps it takes reduce the risk of reidentification or other harm, but it is laughably wrong when is claims that "all data is anonymous and cannot be attached to any individual."[217]

Just like AOL, Phorm associates web surfing history with a unique identifier.[218] Thus, Phorm knows that user number 1337[219] 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. Thus, rather than

---

[211] Ellen Nakashima, *AOL Takes Down Site with Users' Search Data*, WASH. POST, Aug. 8, 2006 at D1.

[212] *Id.*

[213] *Id.*

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

[215] Clayton, *supra* note 78; NebuAd, Inc., Privacy, http://www.nebuad.com/privacy/privacy.php (last visited July 30, 2008).

[216] Clayton, *supra* note 78.

[217] Phorm, Frequently Asked Questions, http://www.phorm.com/about/faq.php [*hereinafter* Phorm FAQ] (partially answering question, "What type of security measures do you have so that aggregated data is not stolen or lost?")

[218] Clayton, *supra* note 78, at ¶ 58.

[219] Phorm identifiers are a sixteen-byte value encoded for humans as a twenty-two character string. *Id.* at ¶ 31. This Article uses shorter numbers for readability.

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

The complexity of Phorm introduces another set of privacy risks.[221] 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.[222] Although this data is eventually thrown away,[223] 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."[224]

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."[225] This does not address entirely 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

---

[220] *Id.* at ¶ 79 (noting that user IDs can be linked to IP addresses at the ISP-run "Profiler" and "Anonymizer" machines).
[221] Id. (listing eighty steps required to serve monitor user behavior and to serve ads).
[222] *Id.* at ¶ 56 (describing data held by "Channel Server," a computer in Phorm's control).
[223] *Id.* at ¶ 58.
[224] Jim Armitage, *Web Users Angry at ISPs' Spyware Tie-Up*, EVENING STANDARD, June 3, 2008.
[225] Clayton, *supra* note 78, at ¶ 80.

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 Service Provider."[226] 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."[227] Perhaps the researcher mistranscribed his list,[228] 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"[229] 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.[230]

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. Because of

---

[226] *Id.*

[227] Phorm FAQ, *supra* note 217 (responding to question "What advertising categories are off-limits?").

[228] 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. 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 which Clayton later corrected in an amended report. http://www.lightbluetouchpaper.org/2008/05/18/twisty-little-passages-all-alike/

[229] Phorm FAQ, *supra* note 217 ("Exclusions are based on Interactive Advertising Bureau (IAB) advertising standards and an in-house editorial panel.").

[230] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 114, at 109 (arguing that "covert surveillance is problematic" because it can "have a chilling effect on behavior.").

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 Part III. Finally, providers can argue that they have received their users' consent. Consent in this context is problematic in ways that will be discussed in Part IV.

B. 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 Part, the Article will survey 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.[231] In the speech, which has become something of a rallying cry for net neutrality advocates,[232] Chairman Powell described four freedoms consumers had come to expect from their ISPs.[233] 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."[234]

Powell's successor, Chairman Kevin Martin, thrust network management even more into the telecommunications policy spotlight through a Commission policy statement[235] declaring that the FCC would

---

[231] Remarks of Michael K. Powell, Chairman of the FCC at the Silicon Flatirons Symposium on "The Digital Broadband Migration" http://www.fcc.gov/commissioners/previous/powell/speeches.html (Feb. 8, 2004).

[232] *See* Testimony of Lawrence Lessig to the Senate Committee on Commerce, Science, and Transportation, Hearing on Network Neutrality (Feb. 7, 2006) ("It is my view that Congress should ratify Powell's 'Internet Freedoms,' making them a part of the FCC's basic law.").

[233] Powell *supra* note 231. The four freedoms are the freedom to (1) access content; (2) use applications; (3) attach personal devices; and (4) obtain service plan information. *Id.*

[234] *Id.*

[235] 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, August 7, 2005, 5:07 PM, http://www.isen.com/blog/2005/08/how-martins-fcc-is-different-from.html.

"incorporate" four principles, modified versions of the four freedoms, "into its ongoing policymaking activities."[236] As a closing footnote elaborated, "[t]he principles we adopt are subject to reasonable network management."[237] 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.[238]

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. The fact that "Comcast was not engaging in reasonable network management," according to the FCC gave grounds for the order to cease throttling BitTorrent[239]

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.[240] These books all struggle to define the precise meaning of the phrase,[241] but they end up defining it in similar ways.[242] This Article adopts one of these definitions: "Network management refers to the activities,

---

[236] Policy Statement in the Matters of Appropriate Framework for Broadband Access to Internet over Wireline Facilities, FCC 05-151 (Aug. 5, 2005) available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.doc.

[237] *Id.*

[238] *E.g.* Electronic Frontier Foundation, *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; Anne Broache, *FCC Wants to Know: Is Degrading P2P Traffic 'Reasonable'?*, CNET, Jan. 15, 2008, http://news.cnet.com/8301-10784_3-9850611-7.html.

[239] FCC Press Release, *supra* note 73, at 2.

[240] BENOIT CLAISE & RALF WOLTER, NETWORK MANAGEMENT: ACCOUNTING AND PERFORMANCE STRATEGIES (2007); ALEXANDER CLEMM, NETWORK MANAGEMENT FUNDAMENTALS (2006); DOUGLAS E. COMER, AUTOMATED NETWORK MANAGEMENT SYSTEMS (2006).

[241] CLEMM, *supra* note 240, at 5 ("As is the case with so many words, *network management* has many attached meanings."); COMER, *supra* note 240, at 26 ("Unfortunately, network management covers such a broad range of networks and activities that no short definition can capture the task well.").

[242] COMER, *supra* note 240, at 26 ("Intuitively, network management encompasses tasks associated with planning, deploying, configuring, operating, monitoring, tuning, repairing, and changing computer networks."); PATRICK CICCARELLI et al., NETWORKING BASICS 386 (2008) ("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."); MANI SUBRAMANIAN, NETWORK MANAGEMENT: PRINCIPLES AND PRACTICE 40 (1999) ("The goal of network management is to ensure that the users of a network receive the information technology services with its quality of service that they expect.")

methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems."[243]

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. But every network management step either involves or must be preceded by a network monitoring event, and because of this Article's central focus on privacy, it will focus on monitoring, and the phrases, "network monitoring" and "network management" will be 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 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[244] and web browsers[245] their visitors use. Network software and hardware vendors survey the applications used on their networks.[246] 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

---

[243] CLEMM, *supra* note 240, at 5.

[244] w3schools.com, OS Platform Statistics, http://www.w3schools.com/browsers/browsers_os.asp (summarizing visitors by operating system used).

[245] Browser News, Browser Stats, http://upsdell.com/BrowserNews/stat.htm (collecting browser studies).

[246] *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).

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."[247] 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."[248] 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.[249]

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 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.[250]

Similarly, in my office at the law school, I run another small network connected to our campus-wide 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.[251] A

---

[247] Cohen, *supra* note 152, at 1402.

[248] *Id.*

[249] 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/CC, Network Situational Awareness (NetSA) Group webpage, http://www.cert.org/netsa/ (last visited July 28, 2008).

[250] SCOTT LOWE, HOME NETWORKING: THE MISSING MANUAL, 3-7 (describing routers designed for home use).

[251] 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, GARTH SNYDER, & TRENT R. HEIN, LINUX ADMINISTRATION HANDBOOK (2006) (measuring 1002 pages).

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.[252]

In order to send my communications to destinations outside their own networks, these ISPs purchase Internet connectivity from larger ISPs. This 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.[253]

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. 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.

From this brief tour, we can divide the world's providers along two axes corresponding, roughly, to the contextual 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. 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*,

---

[252] Some of the University of Colorado's network topology diagrams are posted online. http://www.colorado.edu/its/networking/backbone.html. For a diagram of our wide area network including links to the providers mentioned in the text, see http://www.colorado.edu/its/networking/images/WANConnections.gif.

[253] *See* PRISCILLA OPPENHEIMER, TOP-DOWN NETWORK DESIGN 179 (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.

[254] Some providers are vertically integrated, providing backbone service while selling end-users routing services as well. Speta, *supra* note 19 at 231.

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

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

Turn now to the specific reasons for monitoring. 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.

(1) 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]

(2) 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?

---

[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.COM, Nov. 13, 2007, http://news.cnet.com/Microsoft-exec-calls-XP-hack-frightening/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.COM, Aug. 17, 2004, http://news.cnet.com/2100-7349_3-5313402.html (describing researchers who placed unpatched computers on the network which were compromised in twenty minutes); Honeynet Project, *Know Your Enemy: Statistics*, http://project.honeynet.org/papers/stats/, July 22, 2001 (citing older, similar time-to-exploit statistics).

[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). Internet Engineering Task Force, A Border Gateway Protocol 4 (BGP-4), Request for Comments 4271 (Y. Rekhter et al. eds. Jan. 2006).

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.

Spam and virus filtering come in many forms which 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. 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. 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.[262] 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.

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.[263]

---

[260] Recently, many have tried rigorously to define what an information technology (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), s*ee* Welcome to the Official ITIL Website, http://www.itil-officialsite.com/home/home.asp (last visited July 8, 2008), and the Fault, Configuration, Accounting, Peformance, Security (FCAPS) system, 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 20, 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).

[262] Ohm, *supra* note 125.

[263] *See* Wu, *supra* note 20, at 153 (reporting that when providers bar users from providing content or providing content to the public, "a major goal is bandwidth management.").

They have claimed that mandatory network neutrality will make it impossible for ISPs to cure congestion.[264]

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.[265] 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.

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 email 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 email messages for spam or viruses. It both defies expectations and it 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. At this level, things like spam and viruses are hard to distinguish from other e-mail messages or web surfing behavior.[266]

In order to detect these threats, providers have begun examining much more information, and particularly content information, using automated, always-on deep-packet inspection (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. These tools are like packet sniffers

---

[264] Matthew Lasar, *Martin be Damned, Cable ISPs Want Network Management Freedom*, ARSTECHNICA, July 16, 2008, 5:19 AM CDT, http://arstechnica.com/news.ars/post/20080716-martin-be-damned-cable-isps-want-network-management-freedom.html (paraphrasing two trade association executives warning that "It's going to be Very Bad . . . if 'network management' is denied its unobstructed due. E-mail, Web browsing, online commerce, video and music will be degraded, they promised.").

[265] David Davis, *Clear Up Network Congestion*, TECHREPUBLIC, Nov. 3, 2005, 5:11 PM, http://articles.techrepublic.com.com/5100-10878_11-5930741.html.

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

because they peer deeply in packets, but they are always on, monitoring every packet passing by.

3. Need, Contextual Integrity and the Status Quo

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 about the innumerable risks providers face online. This points to a systematic problem with the theory of contextual necessity: it hitches privacy to the status quo.[267] By identifying privacy through a survey of prevailing norms, Professor Nissenbaum favors past practice over future innovation. She recognizes as much, noting how the theory might be "conservative in possibly deleterious ways."[268] As she puts it, "being so tied to practice and convention loses prescriptive or moral authority."[269]

Nissenbaum proposes a solution to the tendency for her theory to "endorse entrenched flows that might be deleterious,"[270] but it fails to account for dynamic, technology-based privacy conflicts. First, Nissenbaum advises a search for the "historical roots" and "important cultural, social, and personal ends" behind an "entrenched normative framework."[271] She cites medical privacy, which she traces to Hippocrates, and election booth privacy as normative constructs of seemingly ancient heritage.[272]

With conflicts online, however, connections to ancient heritage are drawn only through contestable histories and battles of analogies. Worse, network monitoring is particularly subject to shifting, contingent ethical viewpoints.

After the search for historical roots, Nissenbaum falls back on a costs-benefits balancing, weighing "fundamental values" for and against information flows based on the work of many other scholars.[273] But contextual integrity should provide a way to improve on balancing tests.

There is a better way, which I offer as an improvement to the theory of contextual integrity for online conflicts. There are other sources for finding normative justifications for obeying the status quo or for choosing between alternate versions of the status quo—for establishing the "prescriptive [and] moral authority" as Nissenbaum puts it—aside from ancient history and intramural, philosophical assertions of greater good.

An intriguing possibility is to look at 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

---

[267] Nissenbaum, *supra* note 178, at 143. Other theories of privacy suffer from this same weakness. Professor Surden's theory of evaporating technological constraints favors past constraints over future practice, without adequately providing a roadmap for deciding which constraints we should replicate in law and which we should let fall in the name of progress. Surden, *supra* note 165.

[268] Nissenbaum, *supra* note 178, at 143.

[269] *Id.* at 144.

[270] Nissenbaum *supra* note 178 at 143.

[271] *Id.* at 145.

[272] *Id.* at 145-46.

[273] *Id.* at 147-51.

content of the norms embodied. Professors Mark Lemley and Larry Lessig have argued that engineering design principles, "from the very beginning . . . have been understood to have a social as well as a technological significance. They have, that is, been meant to implement values as well as enable communication."[274]

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.

4. Reasonable Network Management: Provider Need

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. In 1996, Cisco

[274] 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).

created a protocol for network monitoring called NetFlow,[275] building it into its routers ever since.[276] 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."[277]

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. 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; (2) IP destination address; (3) Source port;[279] (4) Destination port; (5) Layer 3 protocol type;[280] (6) Class of Service;[281] and (7) Router or switch interface.[282] 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.[283] 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 on. In a typical session, she accesses her email account several times, reading

---

[275] Cisco Sys. Inc., Introduction to Cisco IOS NetFlow, http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.html (last updated August 2007) *hereinafter* NetFlow Introduction.

[276] http://www.cisco.com/warp/public/146/pressroom/1996/apr96/292.html.

[277] NetFlow Introduction, *supra* note 275.

[278] *Id.*

[279] Ports refer to TCP ports. TCP ports can reveal, to some level of confidence, the application (web, e-mail, IM, etc.) that generated the packet. TCP Ports will be discussed again in Part V.B.

[280] "Level 3" refers to the network layer in both the OSI Reference Model and the Internet Reference Model layers. DOUGLAS E. COMER, 1 INTERNETWORKING WITH TCP/IP: PROTOCOLS AND ARCHITECTURES chapter 10 (5th ed. 2008). Level 3 protocol type will distinguish, for example, between IPv4 and ICMP data.

[281] 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").

[282] 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.

[283] Netflow Introduction, *supra* note 275. 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 (Release 12.1 2001), available at http://www.cisco.com/en/US/docs/ios/12_1/switch/configuration/guide/xcdnfov.html; Cisco Sys. Inc., NetFlow Services Solutions Guide, (Jan. 22, 2007) available at http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/products_implementation_design_guide09186a00800d6a11.html.

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[284] and read twenty.[285] 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.[286] 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,[287] 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 which 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.

---

[284] E-mail is usually sent using the Simple Mail Transfer Protocol (SMTP) protocol, which is usually sent to port 25. IETF, RFC 2821: Simple Mail Transfer Protocol (J. Klensin, ed., July 2001) (defining ESTMP, 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.

[285] If Eleanor uses the older Post Office Protocol Version 3 (POP3) protocol for reading e-mail, the provider might be able to tell only that Eleanor downloaded messages to her computer but might not be able to see how many Eleanor downloaded and read. IETF, RFC 1939: Post Office Protocol—Version 3 (J. Myers & M. Rose, eds. May 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. IETF, RFC 3501: Internet Message Access Protocol—Version 4rev1 (M. Crispin ed. March 2003).

[286] 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 284. 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* § 1.10, http://www.devshed.com/c/a/Administration/Getting-Started-with-Sendmail/12/ (July 7, 2005) (describing sendmail's logging function with default logging of "successful deliveries"); Anton Chuvakian, *Anton Security Tip of the Week #5: Sendmail Log Adventures*, SYSADMIN, Nov. 6, 2005, http://www.oreillynet.com/sysadmin/blog/2006/11/ (showing sample log entry for successful mail delivery under sendmail).

[287] This is through a mechanism known as virtual hosting. BEN LAURIE AND PETER LAURIE, APACHE: THE DEFINITIVE GUIDE 86 (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,[288] 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[289] 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

---

[288] *See* Cristian Estan et al., *Building a Better NetFlow*, 34 ACM SIGCOMM COMPUTER COMM. REV. 245 (2004) ("NetFlow . . . is the most widely used flow measurement solution today."). *But see infra* note 290 (discussing surveys finding surprisingly low usage of NetFlow).

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

than the NetFlow 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 which capture other kinds of data. Some providers do not use NetFlow at all.[290] Despite these true claims, no other form of automated monitoring enjoys the widespread adoption or long history of use as NetFlow.[291]

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 which sets standards for the Internet—has recently begun to develop a protocol for automated network monitoring called IPFIX.[292] After canvassing many alternatives, it selected NetFlow as the model for IPFIX.[293] 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 an exception is carved out for monitoring for incident response, several limits should be enacted to prevent the exception from swallowing the 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

---

[290] Brad Reese, *NetFlow is Not Being Used by 77 Percent of IT Professionals*, NETWORK WORLD'S CISCO SUBNET BLOG, June 23, 2008, 7:55 PM, http://www.networkworld.com/community/node/29224 (reporting results of survey of 600 IT professionals, noting that only 23% of respondents used NetFlow but noting that respondents from larger providers had a higher usage rate). *But see* Cristian Estan et al., *Building a Better NetFlow*, 34 ACM SIGCOMM COMPUTER COMM. REV. 245 (2004) ("NetFlow . . . is the most widely used flow measurement solution today.").

[291] 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.

[292] Internet Engineering Task Force (IETF) IP Flow Information Export (ipfix) Charter (last modified April 23, 2008) http://www.ietf.org/html.charters/ipfix-charter.html.

[293] S. Leinen, RFC 3955: Evaluation of Candidate Protocols for IP Flow Information Export (IPFIX), Oct. 2004.

of incident response for purposes unrelated to the investigation. They should not, for example, be allowed to use the data collected for marketing.

C. 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. Rephrasing this in Nissenbaum's terms, providers might argue that distribution norms can be altered with informed consent.

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.

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. He finds instead that information asymmetries, collective action, bounded rationality, and a lack of meaningful alternatives contribute to what he calls an "autonomy trap."[294]

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."[295] Still, in order to offset "data-processing practices [which] 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."[296] 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 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.

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.

---

[294] Schwartz, *supra* note 196, at 822-23 (2000).
[295] Cohen, *supra* note 152, at 1432.
[296] *Id.*

Dan Solove thinks about privacy "as an aspect of social and legal structure."[297] Neil Richards praises this argument for "shifting the focus of the harms caused by information flow from anecdotal instances of information disclosure to the power implications of those increased flows."[298]

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! mail; or another smaller third-party e-mail provider. 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. They tend also to have many choices for destination providers such as search, news, shopping, and increasingly, video delivery.

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. For these users, there are many similar competitors who do not show contextual advertising. 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. Upstream providers such as Tier 1 providers present no customer choice. A user has no say or even knowledge about the commercial contracts between his 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

---

[297] SOLOVE, DIGITAL PERSON, *supra* note 3 at 97.

[298] Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1096 (2006).

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 which 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 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 which 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 Subpart 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 will focus 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.[299] In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA), amending the law to govern the interception of electronic communications.[300]

a) Few Obvious Answers

As many courts[301] and scholars[302] have complained, ECPA is confusing. The Fifth Circuit has complained that the Act is "famous (if not infamous) for its lack of clarity,"[303] a statement which the Ninth Circuit rejoined "might have put the matter too mildly."[304] Professor Orin Kerr blames this confusion on the unfortunate combination of "remarkably difficult statutory language"[305] and the dearth of cases construing the statute.[306] 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.

---

[299] Omnibus Safe Streets and Crime Control Act of 1968, Pub. L. No. 90-350, 82 Stat. 197 (codified as amended at 18 U.S.C. § 2511-2520).
[300] Pub. L. No. 99-508, 100 Stat. 1848 (codified in various parts of Title 18).
[301] Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994); United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998).
[302] Orin Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805 (2003) ("The law of electronic surveillance is famously complex, if not entirely impenetrable.").
[303] Steve Jackson Games, 36 F.3d at 462.
[304] Smith, 155 F.3d at 1055.
[305] *Id.* at 822.
[306] *Id.* at 823-24.

b) Wiretap Prohibitions

Sniffing packets falls within the prohibited conduct of ECPA and most state wiretap laws. ECPA makes it illegal to "intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept any wire, oral, or electronic communication."[307] An electronic communication is, in part, "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature."[308] 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."[309]

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;[310] to obtain a cookie from a customer's computer;[311] and to install and use spyware to capture chat conversations, instant messages, e-mail messages, and websites visited.[312] 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 wiretapper.[313] 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.[314] Wiretapping is a federal felony investigated by the FBI with a maximum penalty for first-time offenders of five-years in prison.[315]

c) Pen Registers and Trap and Trace Devices Act

The envelope analogy is embedded in ECPA, but not in the way some people think. Some commentators mistakenly claim that it is *legal* to acquire non-content information.[316] On the contrary, although non-content collection falls outside the Wiretap Act's prohibitions, ECPA created a separate law prohibiting the collection of non-content information.

The Pen Register and Trap and Trace Act ("Pen Register Act")[317] regulates the installation and use of devices that "record[] or decode[]" non-

---

[307] 18 U.S.C. § 2511(a)(1).
[308] 18 U.S.C. § 2510(12).
[309] 18 U.S.C. § 2510(4).
[310] United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005) (en banc).
[311] In re Pharmatrak, Inc., 329 F.3d 9, 22 (1st Cir. 2003).
[312] O'Brien v. O'Brien, 899 So. 2d 1133, 1137 (Fla. App. 5 Dist. 2005) (construing state statute modeled after federal wiretap law). *Accord* Potter v. Havlicek, 2007 WL 539534 at *8-9 (S.D. Ohio 2007) (holding use of keystroke and screen shot logging software to be likely ECPA violation).
[313] 18 U.S.C. § 2520(a).
[314] 18 U.S.C. § 2520(c).
[315] 18 U.S.C. § 2511.
[316] 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.").
[317] 18 U.S.C. § 3121 et seq.

content information. 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."[318] 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.

The Pen Register Act is a flawed statute.[319] Most notably, the Pen Register Act has only three statutory exceptions while the Wiretap Act has dozens.[320] 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.[321] 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,[322] and given the lack of prosecutions under this statute—misdemeanor prosecutions tend not to motivate federal law enforcement agents—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 his ethical obligations if he advises his client to violate a criminal law.[323]

d) Stored Communications Act

ECPA also created the Stored Communications Act ("SCA").[324] The SCA restricts access to some communications in storage.[325] ISPs need

---

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

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

[320] *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).

[321] 18 U.S.C. § 2511(2)(g)(i).

[322] Under California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, 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")

[323] *See* ABA, Model Rules of Professional Conduct Rule 1.2(d) (2004).

[324] 18 U.S.C. § 2701 et seq.

[325] 18 U.S.C. § 2701(a).

not worry about this prohibition, however, because unlike the Wiretap and Pen Register Act, ISPs receive blanket immunity under the SCA.[326]

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*,[327] stand for the proposition that a single allegedly wrongful action arises under either the SCA *or* the Wiretap Act, but never under both.[328] The precise reasoning is elaborate, tortured and not worth illuminating fully in this Article.

The most recent court of appeals opinion about this issue refused to follow the misguided *Konop* rule. In *United States v. Councilman*,[329] the First Circuit en banc concluded that an act could be charged under both the SCA and Wiretap Acts.[330]

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.[331] 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,[332] 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

---

[326] 18 U.S.C. § 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.").

[327] 302 F.3d 868 (9th Cir. 2002).

[328] *Id.* at 878. Other cases arguably supporting this conclusion include Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461-62 (5th Cir. 1994) and United States v. Smith, 155 F.3d 1051, 1057 (9th Cir. 1998).

[329] 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.

[330] *Id.* at 82.

[331] Konop, 302 F.3d at 878 n.6

[332] NebuAd's plans have inspired dueling memos debating whether the service violates the Wiretap Act. *Compare* Center for Democracy and Technology, An Overview of the Federal Wiretap 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/headlines/1132 [*hereinafter* CDT Wiretap Analysis] *with* NebuAd, Inc., Legal and Policy Issues Supporting NebuAd's Services, July 8, 2008, http://www.nebuad.com/NebuAdLegalMemo_07_08_08.pdf [*hereinafter* NebuAd Wiretap Analysis].

service," and consent.[333] 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* . . . .[334]

Consider first the permission to protect "rights and property." This exception raises all of the issues of provider need discussed in Part III. This exception does not grant ISPs blanket immunity to conduct any type of monitoring for any reason.[335]

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. As for means, an interception is legal only if it is a "necessary incident" to protecting rights and property.

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

---

[333] 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).

Also, ISPs might invoke the so-called business telephone extension exception. 18 U.S.C. § 2510(4). 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.

[334] 18 U.S.C. § 2511(2)(a)(i) (emphasis added).

[335] Compare the blanket immunity found in the SCA. 18 U.S.C. § 2701(c)(1).

reasonable measures" to address the justification.[336] One court required a "substantial nexus" between the monitoring and the reason for the monitoring,[337] a seemingly more deferential standard, but even that court suppressed some records having nothing to do with the purpose of the investigation.[338]

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.[339] A federal court of appeals refused to apply the exception to a telephone company's taping of conversations in an investigation of theft of service.[340] It ruled, however, that the monitoring of certain non-content information fit within the exception. Extrapolating from 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.[341] 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.

b) "Rendition of . . . Service"

Providers are also entitled to intercept communications as a "necessary incident to rendition of . . . service."[342] 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.[343] For example, long distance operators have been allowed to remain on a line long enough to ensure a

[336] Sistok v. Northern Tel. Sys., 189 Mont. 82, 87 (1980).
[337] U.S. v. McLaren, 957 F. Supp. 215, 219 (M.D. Fla. 1997).
[338] *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.").
[339] Sistok v. Northwestern Telephone Systems, Inc., 189 Mont. 82 (1980).
[340] United States v. Auler, 539 F.2d 642 (7th Cir. 1976).
[341] 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."
[342] 18 U.S.C. § 2511(2)(a)(i).
[343] CARR AND BELLIA, 1 THE LAW OF ELECTRONIC SURVEILLANCE § 3:39 (2008 updates) (summarizing cases).

connection has been established.[344] A motel switchboard operator could overhear conversations while performing duties.[345] A telephone company employee atop a telephone pole in response to customer service complaints could attach his device to the line.[346]

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/bust company which provided free dial-up Internet access to customers willing to watch ads while they surfed.[347]

The problem with allowing providers to broaden this exception to include such specifically-defined services is it turns on difficult factual questions about how a service is marketed, 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 narrow and tightly confined and push this type of analysis to the consent prong.

c) "Consent"

The other exception that may apply to ISP monitoring is the consent exception.[348] 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.C.

Wiretap consent may be express or implied, but implied consent is neither a "reasonable expectation of privacy" test, a test of constructive consent,[349] nor a measure of whether the party simply should have known

[344] People v. Sierra, 74 Misc. 2d 332, 343 (N.Y. Sup. 1973).
[345] U.S. v. Savage, 564 F.2d 728, 731 (5th Cir. 1977).
[346] U.S. v. Ross, 713 F.2d 389 (8th Cir. 1983).
[347] *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).
[348] 18 U.S.C. § 2511(2)(c) (consent by party to the communication "acting under color of law"); § 2511(2)(d) (consent by party to the communication).
[349] In re Pharmatrak, Inc., 329 F.3d 9, 20 (1st Cir. 2003); Williams v. Paulos, 11 F.3d 271, 281 (1st Cir. 1993).

better or had exposed him or herself to some risk of monitoring.[350] 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?[351] 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.[352] Courts instead ask simply, did this particular user receive notice?

In *Williams v. Paulos*[353] the 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,"[354] 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.[355] The Court of Appeals held that without this "minimal knowledge," it would not infer consent.[356]

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. [357] In dictum, 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.[358]

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.[359]

---

[350] Deal v. Spears, 980 F.2d 1153, 1157-58 (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, 2007 WL 539534 at *8-9 (S.D. Ohio 2007) (finding no wiretap consent even though monitored person had "utilize[ed] a computer to which her husband had access and [had used] a "remember me" feature on her email account")..

[351] 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).

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

[353] Williams v. Paulos, 11 F.3d 271 (1st Cir. 1993)

[354] *Id.* at 281 (emphasis added).

[355] *Id.*

[356] *Id.*

[357] In re Pharmatrak, Inc., 329 F.3d 9, 20 (1st Cir. 2003).

[358] *Id.* at 21.

[359] As of 2003, the states that required the consent of all parties to a communication were California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana,

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% 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. 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 specifically sell DPI to Tier 1 providers.[360] These vendors are selling a product that can never legally be used.[361]

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 and the civil verdicts and criminal convictions they suffer will serve as cautionary tales to other providers.

Nevada, New Hampshire, Pennsylvania and Washington. *See* CDT Wiretap Analysis, *supra* note 332, at 11.

[360] Light Reading Industry, *supra* note 51.

[361] These vendors might even be committing a federal crime merely by selling this technology! Section 2512 of the Wiretap Act, which 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).

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 Trap and Trace Device 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.[362] 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 related" 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. 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).[363]

Under the DMCA, it is illegal to circumvent some types of technology used for copyright control.[364] This is why it is likely illegal to copy commercial DVDs, which are protected using a software encryption

---

[362] 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.

[363] 17 U.S.C. § 1201(a)(1)(C) (instructing Librarian of Congress to engage in triennial review to identify persons "adversely affected" by the anti-circumvention provisions).

[364] § 1201(a)(1)(A).

scheme known as DeCSS.[365] 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.[366] 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."[367] 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.[368]

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.

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.[369] 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.[370]

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

---

[365] *See generally* Universal City Studios v. Corley, 273 F.3d 429 (2d Circuit 2001) (discussing DeCSS and the DMCA).
[366] § 1201(a)(1)(C).
[367] *Id.*
[368] Library of Congress & Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protected Systems for Access Control Technologies, 37 C.F.R. Part 201, Docket No. RM 2005-11 (Nov. 27, 2006).
[369] *Cf.* Nat'l Inst. of Standards and Tech., Federal Information Processing Standards Pub. 197, Announcing the Advanced Encryption Standard (AES) (Nov. 26, 2001) (announcing widely-used encryption standard selected by NIST), *available at* http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
[370] *See supra* Part III.C.2 (discussing "in band" communications channels).

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. 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.[371] The principle is based on an economic theory of innovation, which Tim Wu has called "the evolutionary model,"[372] which holds that the preferred path to innovation is through maximizing the number of potential innovators, leading to a "meritocratic" selection of the winners.[373] 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.[374] The three computer scientists who first coined the term have more recently argued that end-to-end maximizes distributed innovation by supporting "the widest possible variety of services and functions, so as to permit applications that cannot be anticipated."[375]

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.[376] Applications which tolerate these problems well (like e-mail) are favored over applications which 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.

---

[371] *See* Tim Wu, *supra* note 20, 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.").
[372] *Id.* at 145.
[373] *Id.*
[374] *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).
[375] David P. Reed, Jerome H. Saltzer, and David D. Clark, *Active Networking and End-to-End Arguments*, 12 IEEE Network 66, 69-71, available at http://web.mit.edu/Saltzer/www/publications/endtoend/ANe2ecomment.html (May-June 1998).
[376] Kyle Dixon et al., *A Skeptic's Primer on Net Neutrality Regulation*, http://www.pff.org/issues-pubs/pops/pop13.14primer_netneut.pdf (working paper of Progress & Freedom Foundation).

A. Flipping the *Status Quo*

There is a close connection between the network neutrality debate and privacy which to date has received little attention.[377] A provider cannot discriminate between packets without scrutinizing them first. If 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* instead.

As providers begin to tiptoe close to the line of discrimination opposed by net neutrality's 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 dollars in remedies for illegal monitoring,[378] 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's 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. 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's 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.

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

---

[377] *See supra* note 10 (listing articles which have touched on the topic).

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

capture the contents of communications. Scrutiny without handling does not violate net neutrality and handling without scrutiny does not necessarily implicate privacy.[379]

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 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 port, which highlights the difference between the two approaches. The TCP port is a number from zero to 65,535 found near the beginning of the packet. TCP ports act as sorting mechanisms for incoming messages; applications "listen" only to particular ports, ignoring packets destined for other ports. 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. A wiretapper can scan the TCP 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 TCP 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. For this reason, TCP port scrutiny worries net neutrality advocates.[380]

From a privacy standpoint, provider scrutiny of a TCP 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.[381] Furthermore, ISPs can make convincing arguments that TCP port scrutiny is necessary in reasonable network management. TCP ports have been logged, for example, in NetFlow from its inception. Tracking traffic by TCP 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.

---

[379] 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 224 and accompanying text.

[380] Wu, *supra* note 20, at 167-68 (listing discrimination by TCP port as something that might cause concern).

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

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.[382] 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 and, thus, bring 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.[383] 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.[384] One company that has emerged as a likely partner is Sandvine.[385] Sandvine is a DPI vendor which sells products that scrutinize packets much more deeply than the TCP port.[386]

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.[387] Sometimes, they clothe these arguments in the language of "freedom," but by this they mean a narrow,

---

[382] *See* Post by ekr to Educated Guesswork blog, Traffic Blocking Evasion and Counter-Evasion, Oct. 29, 2007, http://www.educatedguesswork.org/movabletype/archives/2007/10/traffic_blockin.html.

[383] Eckersley et al., *supra* note 97.

[384] Ernesto, *supra* note 138.

[385] The Consumerist Blog, *Damning Proof Comcast Contracted to Sandvine*, Oct. 27, 2007, 7:34pm, http://consumerist.com/consumer/bittorrent/damning-proof-comcast-contracted-to-sandvine-315921.php.

[386] Sandvine Inc., Solutions Overview, http://www.sandvine.com/solutions/default.asp (last visited Aug. 7, 2008).

[387] *E.g.*, Wu, *supra* note 20; Brett M. Frischmann & Barbara van Schewick, *Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo*, 47 JURIMETRICS 383 (2007). *See also* Christopher S. Yoo, *Network Neutrality and the Economics of Congestion*, 94 GEO. LAW J. 1847, 1851 n.13 (2006) (noting that "network neutrality proponents defend their proposals almost exclusively in terms of the economic benefits of innovation.").

market-drenched conception of freedom.[388] 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.[389] A neutral network is a more private network.

The debate has taken place almost exclusively on insularly 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. Neither side has landed a knock-out punch, however, and both sides admit that their predictions might be wrong.

Thus, Professors Phil Weiser and Joseph Farrell discuss how firms might internalize complementary externalities.[390] Professor Chris Yoo criticizes net neutrality by surveying the economic theory of congestion pricing and devising what he calls "network diversity."[391] Professors Brett Frischmann and Barbara Van Schewick rebut Yoo's theories.[392]

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.

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 Justice Department, a debate about privacy will draw in

---

[388] Ben Scott, Mark Cooper & Jeannine Kenney, Why Consumers Demand Internet Freedom—Network Neutrality: Fact vs. Fiction, May 2006, at 3, *available at* http://www.freepress.net/files/nn_fact_v_fiction_final.pdf.

[389] *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2008).

[390] 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, 101 (2003).

[391] Yoo, *supra* note 387, at 1863-74.

[392] Frischmann & van Schewick, *supra* note 387..

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 in the courts for the first time into the net neutrality debate 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 F.C.C. 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.[393] At the second hearing, Comcast refused to participate at all.[394]

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.

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

[393] Bob Fernandez, *Comcast Admits Paying Attendees at FCC Hearing*, PHIL. INQUIRER, Feb. 28, 2008.
[394] Stefanie Olson, *Absent Comcast in Hot-Seat at FCC Hearing*, CNET NEWS BLOG, Apr. 17, 2008, http://news.cnet.com/8301-10784_3-9921945-7.html.

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."[395] 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.

[395] Staff Study, Permanent Select Committee on Intelligence, U.S. House of Reps., IC21: The Intelligence Community in the 21st Century (April 9, 1996).