University of Illinois Law Review
2009

Article

***1417** THE RISE AND FALL OF INVASIVE ISP SURVEILLANCE

Paul Ohm [FNa1]

***1420** Introduction

Internet Service Providers (ISPs) [FN1] have the power to obliterate privacy online. Everything we say, hear, read, or do on the Internet first passes through ISP computers. If ISPs wanted, they could store it all, compiling a perfect transcript of our online lives.

In fact, nothing in society poses as grave a threat to privacy as the ISP, not even Google, a company whose privacy practices have received an inordinate amount of criticism and commentary. [FN2] Although Google collects a vast amount of personal information about its users, an ISP can always access even more because it owns and operates a privileged network bottleneck, the only point on the network that sits between a user and the rest of the Internet. Because of this fact about network design, a user cannot say anything to Google without saying it first to his ISP, [FN3] and an ISP can also hear everything a user says to any other websites like Facebook or eBay, things said that are unobtainable to Google. The potential threat to privacy from unchecked ISP surveillance surpasses every other threat online.

A potential threat to privacy, however, is not the same thing as a likely invasion, and to distinguish between the two we must make predictions about the future evolution of technology. In this case, the evidence points in opposite directions: on the one hand, historically, ISPs have respected user privacy. [FN4] On the other hand, evolving technology has cast aside hurdles that once prevented providers from monitoring invasively. [FN5]

A deeper look at the evidence shows a numbers of signs all pointing toward a coming wave of more surveillance: online wiretapping used to ***1421** be easy, then it became difficult, and today it is easy again. [FN6] Easier wiretapping has made possible the disintegration of user privacy, while markets have accelerated the trend. [FN7] ISPs are desperately searching for new sources of revenue, and advertisers, technologists, and copyright owners are offering to supply that revenue in return for access to user secrets. [FN8]

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

* * *

I. Privacy Online and How It Is Lost

Not a week seems to go by without the newspapers revealing a new form of invasive ISP monitoring. [FN11] These news stories paint a picture of an industry recently, suddenly, and sharply veering off of a long track record of respect for customer privacy. [FN12] This Part relates some of these developments and offers a few explanations for the sudden change.

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

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

This is a story of means, motive, and opportunity. An ISP's opportunity to invade user privacy stems from network architecture. The ISP operates the network chokepoint--its computers stand between the user and the rest of the Internet--and from this privileged vantage point it has access to all of its users' private communications. The motive to engage in invasive new forms of surveillance comes from many sources, but most importantly, from dire financial need. ISPs, to hear them tell it, are in an industry fighting for survival. In order to increase the revenues the industry***1423** needs to survive, it would like to turn to new forms of moneymaking, most lucratively by selling user secrets for cash. Finally, ISPs only recently have acquired the means to engage in massive and invasive surveillance because surveillance tools have recently become much more powerful; online wiretapping used to be difficult and now it is easy, as demonstrated by a survey of the evolution of computer architecture.

1. Opportunity: Where the ISP Sits on the Network

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

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

In the history of telecommunications law, ISPs are not the first entities with centralized access to all of a customer's communications; telephone companies control similar privileged points of access on the voice network. But, at least since Congress first regulated telephone wiretapping and up to the present day, telephone companies have respected subscriber privacy. Although telephone companies have always had surveillance capabilities, they have tended to listen to conversations only when they have been checking the line, investigating theft of

services, assisting law enforcement, or after receiving the express, time-limited consent of those monitored. [FN13] Telephone companies caught recording in other circumstances have been punished severely for illegal wiretapping. [FN14]

At the same time, largely in line with federal legislation, [FN15] regulation, [FN16] and Supreme Court case law, [FN17] telephone companies have never ***1424** hesitated to collect the non-content information relating to telephone calls: principally who called whom and for how long. Thus, the line between permissible and impermissible telephone monitoring has been drawn through the metaphor of the envelope, with "non-content addressing" information outside the envelope and open to scrutiny and the "content" enclosed within the envelope and off-limits.

Through a set of very important (mostly accidental) circumstances, our privacy online has ended up mirroring the kind of privacy we expect on the voice networks, or at least it had, up until a few years ago. [FN18] From the dawn of the commercial Internet in the mid-1990s until the very recent past, ISPs had respected user privacy, just as their telephone company forebears had, tracking communications in a broad way but not in a deep way.

ISPs have used two modes for monitoring user communications, one broad and noninvasive, the second narrow and invasive. First, ISPs deploy automated computer programs that scrutinize all of the communications--in Internet parlance, the packets--passing through critical points in a network, looking for troublesome communications and acting in response to concerns. Network providers conduct this kind of broad automated monitoring for five reasons: to gauge the health of the network, secure the network, detect spam, detect viruses, and police bandwidth. [FN19] Although automated monitors scan broadly, they are not very invasive because they are discriminating: they tend to ignore content and other information packed, to use another important metaphor, "deeply" within packets. They preserve privacy by keeping a shallow, limited view.

In contrast, ISPs turn to targeted monitoring to respond to incidents. When a network engineer suspects trouble on the network [FN20]--such as a suspected breach of network security by a hacker or unusually heavy congestion on the line--he will often switch on a targeted tool called a packet sniffer, which will peer deeply into packets and store everything it sees.

Compare the relative invasiveness of automated and targeted monitoring. Although targeted monitoring with a packet sniffer invades individual privacy much more than an automated monitor, a packet sniffer ***1425** rarely scrutinizes the data of many users, because it is usually deployed in the network where the information of only a few users can be seen and collected. Thus, automated monitoring protects privacy by "forgetting" much more than it remembers and targeted monitoring by being rare and temporary. Until things began to change not too long ago, most users, most of the time had been subjected only to automated, heavily filtered monitoring. Deep scrutiny was rare. Why did users once enjoy this much privacy, and what has changed?

2. Motive: Extraordinary Pressures

Shifting monetary incentives are the most important forces pushing toward greater ISP surveillance. ISPs have a great motive to pay a little more attention than they have before to their users' secrets. By doing so, they can tap new

sources of revenue, which given their precarious situation, may be the only way they can guarantee their survival.

a. Pressure to Upgrade Infrastructure and Obtain ROI

ISPs are struggling for survival. [FN21] Many economists say the deck is stacked against them. [FN22] 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. [FN23] The result, as one industry analyst puts it, is "accelerated erosion of the revenue per bit earned." [FN24]

Broadband ISPs have responded by searching for new sources of revenue. To this end, they have recognized the emerging market for what I call "trading user secrets for cash," which Google has proved can be a very lucrative market. [FN25]

***1426** b. Google Envy and the Pressure to Monetize

Providers have what some have called "Google envy." [FN26] Google has demonstrated how to grow rapidly by monetizing user behavior, in their case by displaying advertisements matching a users' recent search queries. [FN27] Google's success has redefined expectations for both profitability and privacy online. ISPs trying to replicate Google's performance eye the treasure trove of behavioral data--web transfers, e-mail messages, and instant messages-- flowing through their networks, wondering if they can turn it into advertising money.

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

Another way ISPs might try to forestall the need to invest in expensive network upgrades is to reduce the use of the network. Some users and some applications cause a disproportionate amount of the network traffic, a byproduct of the fact that today ISPs sell service on an all-you-can-eat basis. If they wanted to, ISPs could identify the heaviest users without invading much user privacy by simply counting bytes on a per-user basis. They tend not to take this straightforward and privacy-respecting approach, however, because if ISPs were to cut-off heavy users altogether, they might lose customers and thus revenue. [FN28]

Instead, ISPs have realized that by invading privacy a bit more by tracking and blocking problem applications, they can free up bandwidth without barring any user from using the web and e-mail entirely. [FN29] Through this approach, ISPs can make a few users unhappy but not so unhappy that they will flee to a competitor.

d. Outside Pressures

Increasingly, third parties have exerted a great deal of pressure on ISPs to spy on their users. The recording and motion picture industries view ISP monitoring as an avenue for controlling what they see as rampant infringing activity, particularly on peer-to-peer networks. [FN30]

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 ***1427** Congress to enact the Communications Assistance for Law Enforcement Act (CALEA). [FN31] Under CALEA, providers are obligated to configure their networks to be able to quickly assist law enforcement monitoring. [FN32] Already saddled with the requirements of CALEA, providers may feel ongoing pressure to develop and deploy sophisticated network monitoring tools to help law enforcement stay ahead of surveillance challenges, perhaps out of a sense of civic obligation or to stave off future regulation.

Finally, many providers view new forms of network monitoring as a way to comply with Sarbanes-Oxley, [FN33] Graham-Leach-Bliley, [FN34] Health Insurance Portability and Accountability Act (HIPAA), [FN35] and recent e-discovery changes to the Federal Rules of Civil Procedure. [FN36] Vendors of monitoring products bolster these views by touting their deep-packet inspection (DPI) products as legal compliance tools. [FN37]

* * *

B. Signs of Change

Because ISPs have the means, thanks to recent advances in monitoring technology, motive--financial turmoil coupled with pressures to use new technologies to raise revenue and assist third parties--and opportunity-- ownership of the network bottleneck--they have begun to embrace new forms of aggressive monitoring. In the past year in particular, the headlines have been filled with stories about ISPs conducting or proposing invasive new monitoring. [FN67] This has happened at a breathtaking pace and suggests an undeniable trend.

1. AT&T's Plans for Network Filtering

AT&T's executives have not been shy about their plans to begin monitoring their users in new ways. In 2007, reports emerged that AT&T was in talks with movie studios and record producers to develop new monitoring and blocking technologies. [FN68] In January 2008, during a panel discussion on digital piracy, when asked about the prospect of ISPs using "digital fingerprinting techniques on the network level," an AT&T ***1433** 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." [FN69] Later that month, AT&T CEO Randall Stevenson confirmed that the company was evaluating whether to undertake this kind of monitoring. [FN70]

In 2008, AT&T entered into a new collaboration called Arts + Labs headed by Michael McCurry, the former press secretary under President Clinton, and Mark McKinnon, former media adviser to the younger President Bush. [FN71] Although the mission of the collaboration is still a bit unclear, one can make educated guesses based on the identities of the collaborators, which also include Microsoft; several copyrighted content owning companies like Viacom, NBC, and Universal; and Cisco, the world's leading vendor of networking hardware. [FN72] What all of these parties hold in common is an interest in increased ISP filtering, and McCurry has admitted that the group would try to prevent Congress from enacting new laws prohibiting ISPs from blocking copyrighted material. [FN73]

2. Phorm

A company called Phorm markets a plan for a new method of providing targeted Internet marketing. [FN74] 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. [FN75] By reconfiguring the ISPs' servers, Phorm will be able to access, analyze, and categorize websites users have visited into separate advertising channels. [FN76] If a user visits many travel-related websites, she will begin to see more travel-related ads at Phorm-affiliated websites. [FN77] 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." [FN78]

Because these ads will target to behavior, consumers will be more likely to click on them, justifying higher advertising rates and earning ***1434** more money for Phorm, the ISP, and the website hosting the ad. The potential earnings might be significant; some have suggested that British Telecomm alone will earn eighty-seven million pounds per year from its proposed deal with Phorm. [FN79]

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, [FN80] 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." [FN81] Professor Ross Anderson, an expert in security engineering, said, "The message has to be this: if you care about your privacy, do not use BT, Virgin or Talk-Talk as your internet provider." [FN82] 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. [FN83]

3. Charter Communications and NebuAd

In May 2008, Charter Communications announced its own plan to partner with a company called NebuAd, which sells an advertising model very similar to Phorm's. [FN84] Charter's Senior Vice President sent a letter to customers informing them of the plan and giving them instructions on how to opt out. [FN85]

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. [FN86] Congressmen Edward Markey and Joe Barton wrote a letter to Charter's CEO arguing that the plan might violate federal law and urging the company not to act until it had consulted with Congress. [FN87] ***1435** The Senate Subcommittee on Interstate Commerce, Trade, and Tourism held a hearing about interactive advertising prompted by the controversy. [FN88] Connecticut's Attorney General also released a letter urging Charter not to implement the program. [FN89] In the face of this criticism, about a month after announcing the plan, Charter abandoned it. [FN90] In the meantime, NebuAd has partnered with other, smaller ISPs, some of which have already implemented the program. [FN91] In November 2008, six ISPs and NebuAd were sued by fifteen of their customers seeking to represent a class action of tens of thousands of customers for alleged violation of state and federal privacy laws. [FN92]

4. Comcast Throttles BitTorrent

In August 2007, subscribers to Comcast's cable Internet service began having trouble transferring files using the BitTorrent peer-to-peer protocol. [FN93] Although BitTorrent users had long suspected that ISPs had been slowing down particular types of Internet traffic, Comcast's techniques seemed more aggressive and harder to evade. [FN94] Eventually, the techniques were confirmed by the press [FN95] and activists [FN96] and the Federal Communications Commission (FCC) opened an investigation. [FN97] Throughout the ensuing firestorm, Comcast has repeatedly defended its actions as necessary steps to manage its network. [FN98]

***1436** 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. [FN99] After reports of this behavior emerged, the FCC launched an investigation [FN100] and held two hearings. [FN101]

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. [FN102] 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. [FN103] Specifically, Comcast now plans to manage traffic based on bandwidth usage rather than application choice. [FN104]

On August 1, 2008, the FCC, in an unprecedented and landmark ruling, concluded that Comcast had "unduly interfered with Internet users' rights" and ordered the company to end its discriminatory practices, disclose more details about its practices, and disclose details about its replacement practices. [FN105] Comcast has appealed the ruling. [FN106]

C. Forecast

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

***1437** As further proof of this trend, consider the rise of the DPI industry. [FN107] These companies sell hardware and software tools that consume packets voraciously, like packet sniffers, but monitor at all times, whether or not the ISP has specific cause. [FN108] 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. [FN109] Sales of DPI products in 2007 reached $400 million and are expected to rise to one billion dollars in 2010. [FN110]

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." [FN111] Another vendor, Endace, uses the motto, "power to see all." [FN112]

The "power to see all" will eviscerate user privacy.