The Internet Design Tension between Surveillance and Security

Laura DeNardis
American University

In an effort to examine the protocol design tension between national security interests in surveillance versus network security in the early decades of the Internet and its predecessor networks, this article focuses on one foundational Internet design community, the Internet Engineering Task Force. Cases during this period indicate that the IETF has consistently staked out a consensus position that pushes back against technologically based indiscriminate government surveillance.

After American government contractor Edward Snowden's 2013 disclosures about the expansiveness of National Security Agency (NSA) surveillance practices, Internet protocol designers called for "hardening the Internet" with greater end-to-end encryption.[1] A 2014 consensus "best current practice" document from the Internet Engineering Task Force (IETF) explained that "pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible."[2] The engineering community suggested that extensive and indiscriminate surveillance, whether of protocol metadata or content, presented an assault on individual privacy and that protocol design changes could at least make surveillance "more expensive or infeasible."[3] Later in 2014, the Internet Architecture Board (IAB) issued a statement about confidentiality recommending that encryption be the norm throughout the protocol stack and encouraging protocol designers to make this the default approach to provide confidentiality and to restore trust in the Internet.[4]

Protocols are the standards that enable interoperability and predictable information exchange among computing devices. They are the agreed upon rules providing specifications for formatting, encoding, compressing, error checking, encrypting, and otherwise exchanging information electronically. Routine Internet use relies upon hundreds of these standards, and many of them at various points in history, although not directly visible to end users, have been household names such as Wi-Fi, the MP3 format for digitally encoding and compressing audio, HTTP for communicating between a Web browser and server, voice over IP (VoIP) for Internet voice communications, and the core TCP/IP protocols that have served as fundamental network and transport standards enabling devices to exchange information over the Internet.

Although protocols serve a technical function, they also exist in historically and culturally specific contexts, sometimes establishing public policy such as creating conditions for individual privacy, computer accessibility for the disabled, or global innovation policy. In her 1999 book *Inventing the Internet,* historian of technology Janet Abbate explained that "protocols are politics by other means."[5] Since then, a growing collection of scholarship has explored this theme of the social embeddedness of Internet protocols. Some of these studies address particular standards, such as the geopolitics of Internet Protocol version 6 (IPv6),[6] global power struggles over the security of the Internet's root via DNS Security Extensions (DNSSec),[7] Platform for Privacy Preferences (P3P),[8] the social implications of Domain Name System (DNS) "alternatives,"[9] or the rise of TCP/IP over competing international standards.[10] Other studies more generally examine policy implications of the Internet RFCs,[11] the legal and political implications of Internet standards,[12] and broader historical contexts of Internet governance.[13]

This trajectory of standards research is extended by examining the protocol design

1058-6180/15/$31.00 © 2015 IEEE

tension between national security interests in surveillance versus requirements for network security in the early decades of the Internet and its predecessor networks. This study adopts a broad, yet straightforward definition of surveillance as "the observation or monitoring of an individual's communications or activities."[14] This definition includes both surveillance of content as well as information surrounding content, such as protocol information, packet header, traffic type, and metadata. Surveillance can occur at almost any point in a communication network. Network security protocols refer to the standards enabling services such as authentication (verification of individual or system identity), data confidentiality (protection of data from unauthorized disclosure during transmission over a network), data integrity (assurance that content is not intentionally or unintentionally altered during transmission, and detection and correction of such modifications or errors).[15]

This research project focuses on one foundational Internet design community: the Internet Engineering Task Force.[16] To what extent did the IETF (and its predecessor institutions) address issues related to surveillance and network security in Internet protocol design? More specifically, have Internet engineers pushed back historically against prospects for government surveillance or created conditions enabling surveillance, and if so, what are some cases of protocols that reflected such tensions? From these cases, what further generalizations, if any, can be made about the role of Internet protocol design in public policy debates?

Drawing from primary archival materials—the requests for comments (RFCs) series containing IETF standards and other procedural and information documents, IETF meeting proceedings, personal accounts, and mailing list archives[17]—this study examines approximately two decades, from the formal establishment of the IETF in 1986 through the end of the 20th century, a period that included the first decade of commercial and social Internet changes brought about by the introduction of the World Wide Web but in a political context prior to the September 11, 2001 terrorist attacks on the United States and predating the widespread use of both social media and smartphones.

The overarching findings from this study suggest that the design tension between security and surveillance has existed for decades and that, even as protocol design has continuously evolved and adapted to changing political, socioeconomic, and technological contexts, the Internet engineering community has consistently staked out a consensus position pushing back against technologically based indiscriminate government surveillance. Although this article concentrates solely on 20th century design choices and their intersections with public policy, it may have broader impacts as a historical resource informing contemporary questions about balancing conflicting values of law enforcement, national security, privacy, and network security.

Many early Internet protocols reflected an environment in which security and privacy were not crucial or immediate concerns.

Encryption Strength

Many of the Internet's core protocols emerged in a context quite different from the post-Web Internet. The predecessor networks of what we now call the Internet (such as Arpanet[18] and NSFnet) were noncommercial, significantly smaller, and primarily American, interconnecting a relatively closed ecosystem of trusted communities. Throughout the 1970s and into the 1980s, there was not yet a sense of how globally massive, commercial, or socially enmeshed the Internet would eventually become nor whether core protocols would be widely adopted.[19] In this early context, in which the Internet was used by relatively trusted communities for information exchange and was not yet used for commercial and financial transactions, security was a consideration but not yet a crucial design concern.

On the one hand, many early Internet protocols reflected an environment in which security and privacy were not crucial or immediate concerns. The 1970s Name/Finger protocol provides one early example. The Name/Finger specification was designed to find information about a particular network user, such as an individual's last login information, location, and home phone number. Someone could simply type an individual's email address into a command line interface and receive this information. The specification was documented in RFC 742 in 1977 but invented originally in 1971 by Les Earnest at Stanford.[20] Although participation was voluntary, this protocol helps to convey the climate of familiarity and trust among a much smaller number of network users primarily located in research institutions in the United States.

Another example is the WHOIS[21] protocol (pronounced "who is"). As respected Internet engineer Leslie Daigle (then at Verizon) recounted about the WHOIS protocol, "For historic reasons, WHOIS lacks many of the protocol design attributes, for example internationalization and strong security that would be expected from any recently-designed IETF protocol."[22] WHOIS was originally designed as a white pages type of directory service, a query and response protocol providing an open public record of data on individuals who register a name online. To this extent, the WHOIS system has become the Internet's "surrogate identity system."[23] Illustrating the early 1980s context in regard to real name identification and also one funded and shaped by the US Department of Defense, the 1982 RFC describing the early WHOIS protocol stated that the Defense Communications Agency (DCA) "requests that each individual with a directory on an ARPANET host… be registered in the NIC Identification Data Base," with the registration process including full name, "U.S. mailing address, zip code, and telephone number."[24]

On the other hand, Internet engineers had identified network security as an area of technical focus since at least the first IETF meeting in McLean, Virginia in 1986. The IETF was officially formed that year, although its roots trace back to the technical researchers (including Internet developers Vinton Cerf, David Clark, Steve Crocker, and Jon Postel) working on Arpanet throughout the 1970s. Helping to capture the context of this era prior to the commercialization and globalization of the Internet, the proceedings of the first IETF meeting in 1986 described the proposed mission and establishment of the IETF "to identify and resolve engineering issues in the near-term planning and operation of the DoD Internet,"[25] and over time it was tasked primarily with the development of Internet protocol drafts. This first meeting convened 21 individuals,[26] including Internet engineering pioneers David Clark (MIT), Steve Deering (Stanford), and Robert Hinden (Bolt, Beranek and Newman). Then, as today, the IETF had no defined membership and therefore no formal voting, was made up of individuals rather than institutions, and made decisions based on what later became known as "rough consensus and running code."[27] Nevertheless, one can see the institutional affiliations of individual participants. Those in attendance were primarily American researchers from academic institutions such as MIT, Stanford, and the University of Michigan and defense-related institutions, contractors, and research institutes such as the DCA, Stanford Research Institute (SRI), and Ford Aerospace.

Even in this primarily American, government-funded, and small but growing context, security services were already a design consideration. For example, the proceedings from this first IETF meeting lists "Internet access control and authentication" on its short list of areas of concern in the intermediate term.[27]

The growing commercialization and internationalization of the Internet during this time (and some high-profile security attacks such as the Morris worm in 1988) heightened concern about providing adequate security for commercial and social transactions. This concern was reflected in a debate over encryption strength. Encryption protocols and policies about technologies embedding encryption have historically mediated between law enforcement and national security interests in carrying out surveillance and intelligence gathering activities and socioeconomic requirements for using strong encryption to enable confidentiality, authentication, and data integrity in individual online transactions.[28] At its most basic level, encryption is the scrambling of information prior to transmission to keep it confidential, based on a cipher that encrypts information at its origin and decrypts information at its intended destination. Decryption requires the receiving device to understand the cryptographic algorithm (or cipher) that encrypts the information and also requires knowledge of a key, a binary number needed to begin the decryption process. The length of the binary number, called key length, contributes to the strength of the encryption by determining the relative difficulty of determining the correct decryption key. For example, a standard key length of 128 bits creates a possibility for 2,128 unique keys.

Many cryptographic approaches used in Internet environments actually originated in the

1970s. A prevailing approach was *symmetric-key encryption,* which required the sender and receiver to possess the same encryption key, a technique with the limitation of requiring both parties to have advance knowledge of this common key. In the mid-1970s, Whitfield Diffie and Martin Hellman theorized an approach called *public-key encryption* (or asymmetric encryption) in which each party, rather than using the same common key, uses two distinct keys, a private key no one else knows and a public key anyone can access.[29] To encrypt a message, the sender obtains the receiver's public key, uses it to encrypt the message, and only the receiver's private key is able to decrypt the message encrypted with the recipient's public key. In 1978, three MIT professors (Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman) devised an algorithmic solution to implement public key cryptography, laying the groundwork for Internet security standards for mail (such as S/MIME) and Web transactions (such as TLS), among others.[30] In 1991, computer scientist Phil Zimmerman developed Pretty Good Privacy (PGP), a public-key cryptographic approach used for encrypting files and email. Other public-key encryption approaches originating in the 1990s included Secure HTTP (S-HTTP) and Secure Sockets Layer (SSL).

The functions provided by these public-key cryptography standards help emphasize that encryption is not merely synonymous with confidentiality and privacy of information. Public-key cryptography also serves a variety of information security functions related to authentication, such as certifying the sender's identity, website authentication, or verifying the integrity of transmitted data. For example, public-key cryptography authenticates the identity of a visited website by associating a unique encryption key with that site. In this sense, encryption protocols contribute to a security framework not only related to privacy but also inextricably linked to trust. The ability to trust the Internet for commerce and financial transactions requires a secure information ecosystem able to authenticate online sites as well as protect the privacy of personal information such as credit card numbers and bank account numbers during online transactions. During the 1990s when the Internet increasingly became a platform for commercial and financial transactions, encryption became an essential requirement for securing and authenticating transactions.

At the same time encryption was becoming a necessary precursor for secure online transactions, the mathematically complex arena of cryptographic standards became politicized over collisions between the values of surveillance and values of privacy and commerce. Strong end-to-end encryption enables commerce but prevents, to a certain extent, government surveillance, lawful intercept, or pervasive monitoring for whatever rationale.[31] As such, government authorities have a long history of attempting to legally limit encryption strength, ban types of encryption outright, or enact export controls on encryption.

At the same time encryption was becoming a necessary precursor for secure online transactions, the mathematically complex arena of cryptographic standards became politicized.

Encryption regulations have varied from country to country. In the early 1990s, the United States had an extremely restrictive approach in which encryption was regulated along with firearms under the US International Traffic in Arms Regulations (ITARS). This meant that exporting encryption products required a license; there were prohibitions on exports to countries such as Cuba, Iran, Iraq, and Syria; and the most powerful encryption businesses could legally export, at one point, was 40-bit encryption, fairly easy to break. These restrictions were motivated by concerns for enabling adequate law enforcement and intelligence gathering practices but, despite some exceptions for financial transactions, were increasingly inadequate for protecting commerce. This would potentially affect the global market share of US businesses wishing to sell products based on stronger encryption.

As an indication of the severe regulatory climate related to encryption during this period, in 1993, the US government launched a federal investigation of PGP encryption developer Phil Zimmerman.[32] PGP's encryption strength was considered too high and versions of PGP were available internationally on FTP servers.

At the same time, the rise of the World Wide Web, as historian of technology Paul Edwards has described, seemed "beyond the reach of the Cold War obsession with centralized control" but was "distributed, decentralized, quasi-anarchical, lacking a central purpose or even a main organizer."[33] It was in this context of rapid security technology developments, increasingly decentralized networks, a growing need to secure commercial transactions over the Internet, and the categorization of encryption as munitions under US law that protocol designers weighed in on the debate. In 1993, TCP/IP developer Vinton Cerf gave congressional testimony on the subject.[34] Cerf was asked to give his expert opinion on US policies restricting the exportation of software and hardware implementing certain types of encryption. Cerf suggested, "it seems to me appropriate and timely to reexamine US export control policy" about encryption for various reasons.[34] Encryption products stronger than the products prohibited under US were already available internationally; restrictions were diminishing the global competitiveness of American Internet equipment industries and serving to "inhibit legitimate commerce"; and these restrictions failed to adequately address national security concerns.[34]

The IETF itself tackled this question of security strength at the 32nd IETF meeting held in April 1995 in Danvers, Massachusetts. As an outgrowth of these discussions, the Internet Architecture Board (IAB) and the Internet Engineering Steering Group (IESG) released an informational RFC called "IAB and IESG Statement on Cryptographic Technology and the Internet" (RFC 1984).[35] The IAB is a committee of the IETF with architectural oversight of standards, IETF activities, and appeals.[36] The IESG is an administrative committee made up of the area directors of each IETF working group and the chair of the IETF; the IESG presents Internet drafts to the IAB for consultation as formal Internet standards.

This RFC 1984 was authored by the then-chair of the IAB, Brian Carpenter of CERN in Switzerland, and the then-chair of the IETF, Fred Baker of Cisco Systems, but it put forth a consensus position representing the engineering leadership from the IESG and the IAB. The engineering community acknowledged a dual concern for providing strong security: the requirement for securing international commercial transactions over an increasingly global Internet; and the need to provide privacy for individual Internet users. Sufficiently strong encryption is necessary for fulfilling both of these requirements. RFC 1984 states that the IAB and IESG are "disturbed to note that various governments have actual or proposed policies on access to cryptographic technology" such as export controls, restrictions on key length, requirements for providing decryption keys to governments, and even blanket prohibitions on the use of cryptography.[37] Restrictive government encryption policies were contrary to consumer and business interests and provided only minimal advantages for law enforcement. To summarize the position of RFC 1984, "The IAB and IESG would like to encourage policies that allow ready access to uniform cryptographic technology for all Internet users in all countries."[38]

This consensus position has since been referred to as the Danvers Doctrine.[39] In the context of encryption being legally treated similar to munitions, this free-market position was incongruous and bold but one governments themselves would eventually adopt to a certain extent. In 1996, the United States loosened some of its encryption export regulations, but the tensions between encryption strength and the interests of law enforcement and intelligence gathering practices continued.

The Raven Debate about Wiretapping

By the late 1990s, amongst changing technology and law enforcement contexts, the IETF addressed the question of how it might handle any requests to build "wiretapping" capability into protocols. In 1997, the US Federal Bureau of Investigation had introduced a controversial email wiretapping software program called Carnivore, so the issue of government surveillance of Internet traffic was extant. The specific question of the applicability of wiretapping to Internet protocols emerged in the context of the convergence between the Internet, not yet used for voice telephony, and the public switched telephone network (PSTN), the system of circuit switched networks used for traditional voice calls. A number of IETF working groups were addressing technical aspects of Internet connectivity with the PSTN, or IP-based telephony, and one broached the question of whether they would have to or should design built-in features into protocols to support legal intercept.

Questions about law enforcement/government capability for data surveillance in emerging networks were cropping up globally. Throughout the world, including in the United States, law enforcement agencies expected to, and were legally able to, ask telecommunications providers for information about whom someone was calling, when and for how long the call occurred, and in some cases, the actual audio from a targeted call. The salient questions included how this expectation and capability would translate into the Internet environment, what requirements would be placed on equipment manufacturers, and whether capabilities would be designed into actual protocols.

Lawful communication technology wiretaps had consistently served as a tool for carrying out law enforcement activities in the United States and elsewhere, whether via the telegraph or the phone system. Because telecommunications companies were expected by law to provide this information, manufacturers of switches and other telephony equipment often built this capability into products. Any technical standards for lawful intercept can be vendor neutral while an implementation of standards in a product is vendor specific. In the United States, the Communication Assistance for Law Enforcement Act of 1994 (CALEA) required telecommunication operators to be certain that their networks were capable of complying with legal surveillance of (then) voice calls.[40] The question at hand was whether CALEA would be extended to VoIP and, correspondingly, whether such capability should be standardized in the same way that some telecommunication standards organizations had done for traditional voice telephony.

Wiretapping is an analog term referring to interception via an actual physical connection to a conductor, a technique that is incongruous with how digital environments work. An IETF security glossary from this era defined wiretapping as follows:

> An attack that intercepts and accesses data and other information contained in a flow in a communication system. Although the term originally referred to making a mechanical connection to an electrical conductor that links to nodes, it is now used to refer to reading information from any sort of medium used for a link or even directly from a node, such as gateway or subnetwork switch.[41]

RFC 2804 provides a much more detailed technical definition of wiretapping, although generally suggests that it involves a third party's deliberate capture, filtering, or delivery of information while transmitted from a sending party to a receiving party, unknown to the sender and receiver.

As the IETF explained the context, the organization had "been asked to take a position on the inclusion into IETF standards-track documents of functionality designed to facilitate wiretapping."[42] While this wiretapping question arose in the Media Access Control (Megaco) Working Group[43] in the context of global questions about extending PSTN obligations to the Internet, IETF leadership wanted to broach the subject to the broader Internet engineering community. Thus, the IESG formed a new mailing list, called Raven, designed to discuss the question about possibly creating standards for wiretapping in Internet protocols. At the time, IESG members (again, composed of IETF area directors and the chair of the IETF) included long-time Internet protocol contributors such as Scott Bradner of Harvard, Swedish computer scientist Patrik Faltstrom, and Jeff Schiller of MIT.[44] Fred Baker of Cisco Systems was the chair of the IETF at the time.

The overarching question IETF leadership posed to the broader engineering community was this: "Should the IETF develop new protocols or modify existing protocols to support mechanisms whose primary purpose is to support wiretapping or other law enforcement activities?"[45] In other words, what was the IETF's stance on this issue? The question normatively addressed "should" rather than "how." The question, as posed, took as its starting point that "Adding wiretap capability is by definition adding a security hole" and inquired whether the IETF should diminish Internet security to meet lawful intercept requirements.[45] The questions also sought to sort out how the organization should address country-specific legal contexts as well as anticipate changing legal contexts and to assess how, if it didn't address wiretapping standards, the IETF's image would be construed by various communities, including industry, the Internet community, and national governments.

The deliberations on the Raven email list are archived and available for viewing online.[46] One of the most forceful responses came in the form of "An Open Letter to the Internet Engineering Task Force"[47] from a coalition of 62 individuals from technology companies, universities, computer science organizations, and advocacy organizations. Signers included well-known computer scientists such as Steve Bellovin at AT&T Labs and Whitfield Diffie and Susan Landau at Sun Microsystems, thinkers from advocacy groups such as Alan Davidson at the Center for Democracy and Technology and John Gilmore of the Electronic Frontier Foundation, and academics including Dave Farber at the University of Pennsylvania and Michael Froomkin at the University of Miami (among many others).

> We are writing to urge the IETF not to adopt new protocols or modify existing protocols to facilitate eavesdropping. Based on our expertise in the fields of computer security, cryptography, law, and policy, we believe that such a development would harm network security, result in more illegal activities, diminish users' privacy, stifle innovation, and impose significant costs on developers of communications. At the same time, it is likely that Internet surveillance protocols would provide little or no real benefit for law enforcement.[47]

Their letter also stressed that the IETF was under no legal obligation to develop surveillance protocols. A separate letter from the American Civil Liberties Union (ACLU) stressed that "CALEA, as well as the legislative history, make it quite clear that the Federal government cannot require Internet architecture to be CALEA compliant."[48]

The nature of rigorous debate in the mailing list discussions also reflected a number of normative concerns about engineering ethics, including the prospect of security engineers possibly designing something that diminishes the security of the system. Building in wiretapping features would essentially "amount to designing a security flaw into the system."[49] Many engineers also noted that it would increase the complexity of protocols, which in turn would complicate security. Using protocols to facilitate interception would also create opportunities for non-US interests, such as surveillance on American interests by foreign intelligence agencies or unlawful interception for various criminal activities. Still others suggested that, assuming wiretapping would be mandated and done regardless, there might be advantages for network stability for the IETF to be involved.

After approximately a month of initial mailing list deliberations, the subject was discussed at the November 1999 meeting of the IETF in Washington, DC in a plenary session led by Scott Bradner of Harvard and Jeff Schiller of MIT. The resulting vote (although the IETF does not formally vote, it does gauge a sense of the room) was not unanimous, but it leaned heavily in the direction of rejecting the prospect of building wiretapping into Internet protocols. As Scott Bradner recalled, "We came away with little support for the idea that the IETF should go out of its way to support legal intercept. But at the same time, there was not a consensus that we should prohibit all discussion."[50] Bradner elaborated that "enough people abstained that the IETF could not gauge rough consensus (80% or more) against all such activities."[50] A reporter in the room during the IETF plenary discussion on wiretapping estimated that approximately 25 hands were raised in support of building protocol support for wiretapping, out of roughly 700 to 800 attendees of the plenary.[51] Interestingly, a "sizable portion of the audience refused to state an opinion," meaning they abstained from the vote.[52] This type of organizational deliberation and decision making can seem unusual to those outside the IETF, which does not require unanimity or even formal voting but rather operates under rough consensus.

After the IETF plenary discussion and vote and subsequent discussion in the IAB, the IETF published RFC 2804, "IETF Policy on Wiretapping," in which the IETF (and the IAB and IESG) collectively articulated a position rejecting requests to design wiretapping features into Internet protocols. Stated plainly in its summary position, "The IETF has decided not to consider requirements for wiretapping as part of the process for creating and maintaining IETF standards."[42]

Part of the rationale stemmed from the complex reality of divergent laws on wiretapping (and divergent laws on information privacy, for that matter) across myriad global jurisdictions. The IETF viewed itself as an international standards-setting organization and suggested that jurisdictionally specific design issues were not within its domain.

The IETF position was a further articulation of it position on strong encryption strength and its institutional belief that "both commercial development of the Internet and adequate privacy for its users against illegal intrusion requires the wide availability of strong cryptographic technology."[42]

In retrospect, it is notable that the IETF viewed its policy on wiretapping as not taking a moral position on wiretapping. For example, RFC 2804 stated:

> Much of the debate about wiretapping has centered around the question of whether wiretapping is morally evil, no matter who does it, necessary in any civilized society, or an effective tool for catching criminals that has been abused in the past and will be abused again. The IETF has decided not to take a position in this matter.[53]

If the IETF had decided to standardize wiretapping capability into protocols, this would likely have been construed as taking a moral position, certainly as indicated in the mailing list archives discussing this issue. While the topic of lawful interception and Internet protocols would continue to emerge,[54] the Raven debate and RFC 2804 served as a preemptive rejection of a coordinated effort to build lawful intercept capability into the Internet's protocols. This policy position did not, by extension, mean that individual companies, such as router manufacturers, should not be required, under CALEA in the United States or by various laws in other countries, to build lawful intercept capability into products. What it did suggest was that there should not be an industry-wide standardization effort to harmonize such capabilities.

The Rejection of Physical Identifiers in IPv6 Addresses

Security and surveillance concerns also converged when the Internet engineering community worked on a new protocol to replace the long-prevailing standard for Internet Protocol (IP) addresses, Internet Protocol version 4 (IPv4). IP addresses are the globally unique number identifiers devices use to communicate over the Internet, somewhat analogous to a postal address, only virtual rather than physical and assigned either permanently or temporarily for a session. The IPv4 standard assigned 32 bits (32 zeros or ones) to each address, providing a global pool of 2^{32}, or roughly 4.3 billion addresses.[55] This number was optimistic and insightful in the early 1980s context in which the protocol was published and seemed to assume that the network could grow dramatically. But by 1990, engineers identified the potential exhaustion of this address pool as a crucial design concern and embarked on a new IP standard that would significantly expand the address space.

The protocol IPv6, ultimately selected to replace IPv4, extended the length of each address from 32 to 128 bits, supplying 2^{128}, or 340 undecillion addresses. In determining details of the IPv6 specification, engineers grappled with a design question that intersected directly with privacy. The original IP standard specified that each address would be a virtual identifier, meaning not tied directly to a physical hardware number or other physical identifier. Even though Internet addresses, even as virtual identifiers, later became part of a larger identity infrastructure that fed into systems of data collection for surveillance, law enforcement, and online advertising, the virtual identification feature provided much more privacy than a physical identifier. The address appended to information transmitted over the Internet is software defined rather than associated with any physical architectural component.

Since the first hints of Internet commercialization and internationalization, the IETF has served as a force resisting protocol-enabled surveillance features.

In designing IPv6, questions emerged about how a 128-bit IPv6 address would be derived. One approach under consideration involved embedding a computer's hardware serial number into some IPv6 addresses, an approach that would shift Internet addresses from purely logical identifiers to physical identifiers, conceivably enabling information transmitted over the Internet to be traced to a specific computing device and therefore traced to a physical location and possibly an individual's identity.[56] This is an oversimplification of the technological choices at hand, but the physical identifier potentially embedded into the Internet address could most accurately be described as an Ethernet address, a 48-bit binary number associated with an Ethernet card and used for local area network transmission.

The engineering community debated the privacy implications of various address structures and ultimately rejected the direct incorporation of a physical identifier into an IPv6 address and instead built in privacy protections/extensions into the design of IPv6.[57] Much of the debate occurred in 1999, after a decade of rapid Internet growth and commercialization that introduced new Internet companies like Amazon, eBay, Google, Yahoo and PayPal, and in the peak year of the Internet dot-com boom. A hardware identifier built into an IP address would have facilitated, or at least enhanced, the personal identity infrastructure around surveillance in the context of this rising everyday Internet use. At the same time, and also related to privacy protection, the IETF initially mandated support for a network-layer encryption protocol called IPsec into IPv6.[58] Both of these contexts emphasize design concerns about security and privacy protection and, by extension, creating conditions that complicate prospects for surveillance.

Protocols as One Component of Public Policy

While hardly exhaustive, these cases suggest that, since the first hints of Internet commercialization and internationalization, the IETF has supported strong security in protocol design and has sometimes served as a force resisting protocol-enabled surveillance features. When the IETF responded to NSA surveillance disclosures with a consensus statement describing pervasive monitoring as an attack that should be addressed in protocols, this position did not materialize in a vacuum but rather followed a long trajectory of tensions between network security and efforts to facilitate surveillance. Rationales for strong security have both been commercially motivated and motivated by concerns for individual privacy rights.[59]

These cases also support the thesis that standards are sometimes spaces in which technical policy and social policy converge. Contextual factors—whether economic, political, or social—shape technical design decisions.[60] The public interest implications of protocol design also raise questions related to Internet governance. Although outside the scope of this article, an accompanying question is, what are the procedural and participatory conditions that legitimize this form of public policy making, not by traditional nation states or intergovernmental organizations, but by new global institutions comprised primarily of individuals working in private industry? Part of this legitimacy comes from the IETF's procedural and informational openness as well as its expertise and track record. The IETF's standards-setting approach is open and transparent in several respects.[61] Anyone may participate in its activities, and there is no formal membership. Unlike some other standards organizations, the organization openly and freely publishes its standards and gives preference to standards with no embedded intellectual property rights, a feature that has helped to promote Internet innovation by allowing for multiple competing products based on these standards.

What these cases also allude to is that protocols in themselves do not resolve social debates. Standardization is a foundational part of the Internet ecosystem but only one part. For example, wiretapping can still be built into switches, with or without standardization. Information intermediaries can still hand over personal information to governments. Through an engineering lens, surveillance is not a monolithic practice. It can involve cracking the encryption keys securing protocols, using invasive tools that can access the content contained in packets, conducting network traffic analysis, or monitoring the metadata surrounding content. Even in cases in which protocol design establishes a form of public policy, it is important to note that a protocol specification does not automatically translate into protocol implementation or even usage.

The broader Internet governance ecosystem, including laws, international agreements, and business practices, presents additional opportunities to address surveillance. Efforts that call upon Internet engineers to push back against surveillance sometimes overlook these other layers of Internet governance. What complicates these many levers to potentially respond to surveillance is that there are many motivations for carrying out "surveillance." It is not a monolithic practice. The same exact pervasive monitoring techniques can be used for foreign intelligence gathering, domestic surveillance, lawful interception, data collection and retention to support business practices based on customized online advertising, the performance of routine network management functions, or the detection of security problems such as viruses, worms, spam, and distributed denial of service (DDoS) attacks. Public concern about expansive government surveillance does not necessarily translate into similar concerns about the data collection and sharing practices of Internet companies to support business models based on online advertising.

Finally, technical design itself is malleable. Internet architecture is not fixed but is constantly evolving and adapting to new uses, new innovation, new economic opportunities, and changing cultural norms. Because usage contexts and technological innovation are constantly changing, protocols also evolve. Internet designers adapt to these changing contexts and new challenges. Hence, in the context of responding to information about the expansiveness of NSA surveillance, the IETF suggested, "It is therefore timely to revisit the security and privacy properties of our standards."[62]

Acknowledgments

The author acknowledges the helpful comments from Thomas Misa, Jeffrey Yost, Pindar Wong, the anonymous reviewers, and the participants in the National Science Foundation (NSF) funded Computer History Workshop at the Charles Babbage Institute at the University of Minnesota.

References and Notes

1. "Hardening the Internet" was the title of the Technical Plenary of the IETF 88 meeting of the Internet Engineering Task Force in Vancouver, Canada, in Nov. 2013.
2. S. Farrell and H. Tschofenig, *Pervasive Monitoring Is an Attack*, IETF RFC 7258, May 2014; www.rfc-editor.org/rfc/rfc7258.txt.
3. Farrell and Tschofenig, p. 1.
4. "IAB Statement on Internet Confidentiality," 14 Nov. 2014; https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/.
5. J. Abbate, *Inventing the Internet*, MIT Press, 1999.
6. L. DeNardis, *Protocol Politics: The Globalization of Internet Governance*, MIT Press 2009.
7. B. Kuerbis and M. Mueller, "Securing the Root," *Opening Standards: The Global Politics of Interoperability*, L. DeNardis, ed., MIT Press, 2011.
8. A. Davidson, J. Morris, and R. Courney address the public interest implications of P3P and several other Internet standards debates in "Strangers in a Strange Land: Public Interest Advocacy and Internet Standards," 30th Telecomm. Policy Research Conf., Sept. 2002.
9. F. Musiani, "Decentralizing DNS: Peers, Infrastructure, and Internet Governance," *Georgetown J. Int'l Affairs*, vol. 15, no. 1, article gj13010.
10. A.L. Russell, *Open Standards and the Digital Age: History, Ideology and Networks*, Cambridge Univ. Press, 2014; A.L. Russell, "'Rough Consensus and Running Code' and the Internet-OSI Standards War," *IEEE Annals of the History of Computing*, vol. 28, no. 3, 2006, pp. 48–61.
11. See, for example, S. Braman, "Internet RFCs as Social Policy: Network Design from a Regulatory Perspective," *Proc. Am. Soc. Information Science and Technology*, vol. 46, no. 1, 2009, pp. 1–29.
12. For example, L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, 1999; J. Palfrey and U. Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems*, Basic Books 2012.
13. Examples include M. Mueller, *Networks and States: The Global Politics of Internet Governance*, MIT Press, 2010; L. DeNardis, *The Global War for Internet Governance*, Yale Univ. Press, 2014; and E. Brousseau, M. Marzouki, and C. Meadel, eds. *Governance, Regulation and Powers on the Internet*, Cambridge Univ. Press, 2012.
14. A. Cooper et al., *Privacy Requirements for IETF Protocols*, IETF RFC 6973, July 2013; www.rfc-editor.org/rfc/rfc6973.txt.
15. J. Schiller, *Strong Security Requirements for Internet Engineering Task Force Standard Protocols*, IETF RFC 3365, BCP 61, Aug. 2002, p. 2; www.rfc-editor.org/rfc/rfc3365.txt.
16. Other examples of technical standards-setting institutions include the World Wide Web Consortium (W3C), IEEE, the International Telecommunication Union (ITU), the Standardization Administration of China (SAC), and the American National Standards Institute (ANSI), just to name a few.
17. The Internet's request for comments (RFC) series are (now) electronic archives that, since 1969, have documented Internet standards, governance procedures and institutional responsibilities, and other information related to Internet protocols and the work of the IETF and its predecessor organization the IAB. The more than 6,000 RFCs offer both a technical and social history of proposed standards, final Internet standards, and opinions from Internet pioneers and current leaders. The RFC archives are available online at www.rfc-editor.org. The IETF also publishes meeting proceeding archives (throughout its history since 1986). The IETF holds three annual meetings. These gatherings have grown from 21 attendees in 1986 to more than 1,000 participants. The IETF provides electronic archives of extensive proceedings and minutes from the IETF plenary and breakout sessions at www.ietf.org/meeting/proceedings.html. This project also relies upon IETF mailing list archives. The RFCs, whether informational or actual Internet standards, are usually the end result of much deliberation and discussion on mailing lists. These mailing lists often contain the back story about relevant issues, how decisions were made, and what potential conflicts ensued. The IETF's electronic mailing list archives (including discussion lists, announcement lists, and working

group lists) are available at https://www.ietf.org/list/. As a more specific example, the IETF Raven mailing list archives are available at www.ietf.org/mail-archive/web/raven/current/thrd2.html#00737.

18. The Arpanet was a US-government contracted packet switched network built in the early 1970s that is considered the predecessor network that led to the Internet.
19. A.L. Russell, "OSI: The Internet That Wasn't," *IEEE Spectrum*, 30 July 2013; http://spectrum.ieee.org/computing/networks/osi-the-internet-that-wasnt.
20. K. Harrenstien, *Name/Finger*, IETF RFC 742, Dec. 1977; www.rfc-editor.org/rfc/rfc742.txt.
21. WHOIS is not an acronym but short for "who is."
22. L. Daigle, *WHOIS Protocol Specification*, IETF RFC 3912, Sept. 2004, p. 1; www.rfc-editor.org/rfc/rfc3912.txt.
23. M. Mueller and C. Mawaki, "Disrupting Global Governance: The Internet Whois Service, ICANN, and Privacy," *J. Information Technology & Politics*, vol. 5, no. 3, 2008, pp. 303–325. In the era after the introduction of the World Wide Web, for example, this data recorded personal information about an individual associated with the registration of an individual's domain name. Accredited registrars, the companies (such as GoDaddy) that sell domain name registrations, collect this information when someone applies for and purchases a domain name and make this information freely searchable and available online via the WHOIS system.
24. K. Harrastien and V. White, *NICNAME/WHOIS*, IETF RFC 812, Mar. 1982; www.rfc-editor.org/rfc/rfc812.txt. Obsoleted by K. Harrenstien et al., *NICNAME/WHOIS*, IETF RFC 954, Oct. 1985; www.rfc-editor.org/rfc/rfc954.txt.
25. IETF 1, proceedings of the first IETF meeting, then called the meeting of the "DARPA Gateway Algorithms and Data Structures Task Force Meeting," Jan. 1986, p. 9; www.ietf.org/proceedings/01.pdf.
26. The IETF's first meeting had 21 participants, but this swelled to roughly 1,500 per meeting only 10 years later in 1996, illustrating the growing interest in the Internet.
27. A term deriving from David Clark's plenary presentation, "A Cloudy Crystal Ball, Visions of the Future," *Proc. 24th Internet Eng. Task Force*, 1992, p. 539.
28. See, for example, accounts of these tensions in W. Diffie and S. Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, 1st ed., MIT Press, 1998; S. Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, MIT Press, 2013.
29. W. Diffie and M.E. Hellman, "New Directions in Cryptography," *IEEE Trans. Information Theory*, vol. 22, no. 6, 1976, pp. 644–654.
30. R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Comm. ACM*, vol. 21, no. 2, 1978, pp. 120–126.
31. D. Clark and M. Blumenthal, "The End-to-End Argument and Application Design: The Role of Trust," *Federal Comm. Law J.*, vol. 63, no. 2, 2011, pp. 357–390.
32. US government charges against Zimmerman were dropped in 1996.
33. P. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America*, MIT Press, 1996, p. 354.
34. As a follow-up to his March 1993 congressional testimony before the Subcommittee on Technology, Environment and Aviation, V. Cerf, "Letter to the Honorable Timothy Valentine, Committee on Science, Space and Technology, U.S. House of Representatives," 11 Apr. 1993, http://cpsr.org/prevsite/program/clipper/cerf-letter-to-congress.html.
35. Internet Architecture Board (IAB) and Internet Engineering Steering Group (IESG), *IAB and IESG Statement on Cryptographic Technology and the Internet*, IETF RFC 1984, Aug. 1996; www.rfc-editor.org/rfc/rfc1984.txt.
36. For more information, see the overview of the IAB at https://www.iab.org/about/iab-overview/.
37. RFC 1984, p. 1.
38. RFC 1984, p. 2.
39. J. Schiller, *Strong Security Requirements for Internet Engineering Task Force Standard Protocols*, IETF RFC 3365, BCP 61, Aug. 2002, p. 3; www.rfc-editor.org/rfc/rfc3365.txt.
40. S. Landau, "CALEA and Network Security," *IEEE Security & Privacy*, vol. 3, no. 6, 2005, pp. 26–33. See also A.M. Froomkin, "Habermas@discourse.net: Toward a Critical Theory of Cyberspace," *Harvard Law Rev.*, vol. 113, no. 3, 2003, pp. 749–873.
41. R. Shirey, *Internet Security Glossary*, IETF RFC 2828, May 2000, p. 191; www.rfc-editor.org/rfc/rfc2828.txt.
42. *IETF Policy on Wiretapping*, IETF RFC 2804, May 2000; www.rfc-editor.org/rfc/rfc2804.txt.
43. According to a posting by Scott Bradner, the question arose in the Media Access Control (Megaco) Working Group (see www.ietf.org/mail-archive/web/raven/current/msg00002.html).
44. An archive of IESG members and IETF chairs in each year is available at www.ietf.org/iesg/past-members.html.
45. IESG posting on IETF-Announce mailing list, "[Raven] The IETF's Position on Technology to Support Legal Intercept," 11 Oct. 1999; www.ietf.org/mail-archive/web/raven/current/msg00000.html.

46. For Raven mailing list archives, see www.ietf.org/mail-archive/web/raven/current/mail2.html#00754 and www.ietf.org/mail-archive/web/raven/current/maillist.html.
47. See "An Open Letter to the Internet Engineering Task Force," 10 Nov. 1999; www.ietf.org/mail-archive/web/raven/current/msg00733.html.
48. See mailing list posting at www.ietf.org/mail-archive/web/raven/current/msg00664.html.
49. J. Zittrain, "ICANN: Between the Public and the Private Comments before Congress," *Berkeley Technology Law J.*, vol. 14, 1999, pp. 1070–1094, note 20. See also J. Morris, H. Tschofenig, and J. Peterson, "Policy Considerations for Internet Protocols," IETF Internet draft, Oct. 2010, p. 15; https://tools.ietf.org/id/draft-morris-policy-cons-00.txt.
50. S. Bradner, "When in Washington…," Net Insider Column, *Network World*, 22 Nov. 1999, p. 44.
51. See *Wired* reporter Declan McCullagh's posting on cyberia-L@listserve.aol.com, 13 Nov. 1999. Accounts on the IETF's Raven mailing list suggested there were more than 1,000 in the room.
52. RFC 2804, p. 3.
53. RFC 2804, p. 5.
54. See, for example, S. Bellovin et al., "Going Bright: Wiretapping without Weakening Communications Infrastructure," *IEEE Security & Privacy*, vol. 11, no. 1, 2013, pp. 62–72.
55. J. Postel, *Internet Protocol, DARPA Internet Program Protocol Specification Prepared for the Defense Advanced Research Projects Agency*, IETF RFC 791, Sept. 1981; www.rfc-editor.org/rfc/rfc791.txt
56. For a historical account of these design choices, see L. DeNardis, "Architecting Civil Liberties" *Protocol Politics: The Globalization of Internet Governance*, MIT Press, 2009, pp. 71–96.
57. T. Nartin et al., *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, IETF RFC 4941 (obsoletes RFC 3041), Sept. 2007; www.rfc-editor.org/rfc/rfc4941.txt.
58. The initial IPv6 mandate of the inclusion of IPsec was later changed to a recommendation that it should be included. See, for example, E. Jankiewicz, et al., *IPv6 Node Requirements*, IETF RFC 6434, Dec. 2011; www.rfc-editor.org/rfc/rfc6464.txt.
59. For a more recent statement, see A. Cooper et al., *Privacy Requirements for IETF Protocols*, IETF RFC 6973, July 2013; www.rfc-editor.org/rfc/rfc6973.txt.
60. See, for example, H. Hochheiser, "Indirect Threats to Freedom and Privacy: Governance of the Internet and WWW," *Proc. 10th Conf. Computers, Freedom, and Privacy*, 2000, pp. 249–254, Davidson, Morris, and Courney, "Strangers in a Strange Land," 2002; and S. Braman, "The Geopolitical vs. the Network Political: Internet Designers and Governance," *Int'l J. Media and Cultural Politics*, vol. 9, no. 3, 2013, pp. 277–296.
61. See, for example, L. DeNardis, "The IETF as an Open Institution," *Protocol Politics: The Globalization of Internet Governance*, MIT Press. 2009, p. 223.
62. RFC 7258, p. 3.

Laura DeNardis is a professor in the School of Communication at American University in Washington, DC. She is a fellow of the Yale Information Society Project and previously served as its executive director. She is a senior fellow of the Center for International Governance Innovation (CIGI) and the research director for the Global Commission on Internet Governance. DeNardis has a PhD in science and technology studies from Virginia Tech. Contact her at denardis@american.edu.