Georgia Tech School of Public Policy

STANDARDIZING SECURITY:
Surveillance, Human Rights, and TLS 1.3

MILTON L MUELLER AND COLIN J KIERNAN

SUMMARY

This paper conducts a detailed case study of the development of a new transport layer security (TLS) standard and its implications for the privacy of Internet users and the security and accountability of network operators. TLS version 1.3 was developed by the Internet Engineering Task Force (IETF) from 2014 - 2018 in reaction to a major political controversy over surveillance. Analyzing the controversies around its design, adoption and implementation illuminates the role of technical standards in the governance of cybersecurity and the Internet. It also contributes to an ongoing theoretical debate about the degree to which protocols or standards can be considered "political." The paper develops a conceptual framework that identifies three distinct relationships between standards and political/social effects: 1) the political economy of the standardization process (PES); 2) the societal effects of a standard's adoption, implementation and use (SES); and 3) protocols have politics (PHP), or politics and rights are embedded in the standard. In analyzing the development of TLS 1.3, we find that the PHP approach had limited explanatory value compared to the first and second approaches. By conveying the idea that political, economic and social effects can be hard coded into protocol designs, the protocols-have-politics view short-circuits careful analysis of the way standards contribute to governance.

INTRODUCTION

This paper is a detailed case study of a new technical standard, and the subsequent contention over its impact on the privacy of Internet users and the security and accountability of network operators. The protocol in question is known as Transport Layer Security version 1.3 (TLS 1.3). TLS 1.3 was published as a formal standard by the Internet Engineering Task Force (IETF) in August 2018. [1] Its development was inspired by Edward Snowden's revelations of mass surveillance by the U.S. government. By strengthening the confidentiality of Internet communications, the standard was supposed to prevent the kind of mass surveillance that Snowden exposed.

The Internet is known for its distributed decision making and crossing of jurisdictional boundaries, which makes traditional forms of communications governance more difficult and complex. The production and implementation of technical standards can be considered an important arena where the global governance of cybersecurity takes place. An examination of the interactions of standards development organizations (SDOs), privacy advocates, government intelligence and law enforcement agencies, and private network operators in critical sectors such as banking clarifies the complex mechanisms by which policy goals such as cybersecurity and privacy are achieved on the global internet.

The story of TLS 1.3 also contributes to an ongoing theoretical debate about the degree to which protocols, standards, or technologies "embody" politics or values. [2] [3] In this debate, it is not uncommon to encounter claims that "protocols are political" [4], that "protocols have politics" [5] or that "protocols are politics by other means" [6]. There is also a burgeoning literature on values in design, which suggests that desired behavior in society can be encouraged or even enforced by means of design choices in information systems. [7] [8] [9] [10] The case of TLS 1.3 creates the opportunity to critically examine these claims about the political or value-laden nature of protocols.

The thesis of this paper is that the protocols-have-politics claim provides limited insight into the relationship between technical standards and Internet governance. By conveying the idea that political, economic and social effects are somehow "baked into" a protocol design, it can short-circuit analysis of the real ways in which standards/protocols lead to societal effects; if taken literally, it can mislead observers about the amount of leverage over governance one can obtain by getting a standard through an SDO.

To support this thesis, we provide both a conceptual framework and empirical evidence in the form of a detailed case study. Our conceptual framework identifies three different ways in which protocols or standards might affect governance and politics, untangling methods of influence that are often conflated, confused or poorly defined. We then examine the standardization and implementation of TLS 1.3 in detail. That account shows that while the design of the protocol was intended to support stronger privacy, TLS 1.3 encountered numerous obstacles to and limitations upon its intended social impact. We conclude that the real politics and effects are not "in" the protocol itself, but in the stakeholder groups who contended over the design, adoption and implementation of the new standard.

We define the terms "protocols" and "standards" as follows. In data communication the term "protocol" denotes a sequence of rules or instructions for the formatting and exchange of data that are agreed upon by developers to achieve compatibility. These agreements are specified in a formal standards document by a Standards Development Organization and implemented in the design of the software, firmware and/or hardware supporting information systems. TLS 1.3 in particular is a transport-layer *protocol* that has been *standardized* by the IETF RFC 8446, so one can refer to it as either a standard or a protocol.

GOVERNANCE, PROTOCOLS AND POLITICS

What we call "the" Internet is a transnational network of independently administered networks using compatible protocols. Authority over its operations is distributed; the Internet as a whole cannot be subjected to any central authority's control. This fact has led to various institutional innovations and experiments with new forms of governance. [11] Technical standards are widely recognized as one of the mechanisms of Internet governance. [12] [13]

In recent years, however, the recognition that standards play a role in shaping Internet governance has morphed into a stronger and more ideological claim that protocols actually *have* politics or values embedded in them. [4] This claim has important implications for SDOs and for Internet governance. But it is hampered by a lack of clarity. The definition of "politics" in this claim is often unclear, or so broad as to include any kind of social shaping, whether intentional or unintentional, short-term or long-term. Its adherents routinely conflate the design of a standard with its adoption and implementation.

The following conceptual framework for analyzing the relationship between standards and politics can help to clarify discussion and analysis. Our framework identifies three distinct positions one might take on how protocols and politics or governance are related. We refer to them as the Political Economy of Standardization (PES), the Societal Effects of Standards (SES) and Protocols Have Politics (PHP).

1: The political economy of standardization (PES)

At its simplest, protocol politics can mean that the formal specification of protocols in documents reflects a set of interactions, bargains and compromises among a group of interested actors. The process can plausibly be called *political* because a standardized protocol, like an institution, represents an equilibrium bargain amongst a set of engaged stakeholders. [14] The stakeholders are likely to be competing technology vendors, government agencies, user groups and sometimes civil society advocacy groups. The standard they ultimately agree upon reflects the interests, ideas, participation and bargaining strength of the different actors. If one looks at protocol politics in this way, one must carefully examine the compromises and bargains that went into its development, and how the technical choices being considered are related to the interests of the actors. But in this approach the protocol is an *outcome* shaped by the political (and economic) interests of the participants in the standardization process; it is the participants who have politics and interests, not the protocol.[1] In this regard, practically every social phenomenon is 'political' (and economic). Just as there are office politics affecting decisions and choices in an organization, so there are politics underlying the development of a protocol in an SDO. Rather than saying protocols *have politics* one should rather talk about the *politics of standardization;* or, given the prominence of business considerations, the *political economy* of standardization (PES).[2] PES is not new; scholars have been doing it for the past 40 years at least [15] [16] [17].

[1] Take the famous case of the size of the packet in asynchronous transfer mode (ATM) protocol. Some engineers wanted smaller packet sizes (32 octets) to make the system more suited to streaming voice, while other engineers wanted larger packet sizes (64 octets) to make the system more suited to data. The factions behind these positions roughly corresponded to U.S.-based "net-heads" rooted in the Internet community and Europe and Japan-based "bell-heads" with roots in the telephone companies. The ultimate size of the packet that was agreed – 53 octets – was, famously, an arbitrary middle ground, a bargain that inspired scorn among purists. In this sense the protocol reflected a political stalemate. But it would be hard to demonstrate that this equilibrium imposed or embedded certain political distributions or values on society as a whole.

[2] *Politics* connotes power to compel or influence societal outcomes, usually via governmental institutions, whereas *economics* deals with the monetary benefits at stake and the way costs and benefits are distributed among the actors. Although politics and economics are distinguishable, power can confer economic benefits and wealth can help to confer power, so the term "political economy" reflects both their interdependence and their separateness.

2: Societal Effects of Standards (SES)

A second position would be to examine how society as a whole is affected or shaped by a protocol once it is put into use. An SES approach recognizes that standards, when implemented, constrain and structure society in certain ways. This may be due to their differing affordances [18], or it may reflect their impact on the distribution of economic and political benefits [19], e.g., through the presence of intellectual property over relevant technologies, or the creation of compatibility relationships that empower specific businesses or governments. The claim that standards or protocol designs have societal effects is consistent with the observation that stakeholders invest significant resources in developing and promoting them. It implies that when competing or alternative standards are present, social outcomes will be different if one of them is implemented and the other isn't. Understanding societal impact, however, requires a different type of analysis than PES as described above – and it is far more difficult. To appraise societal impact one must examine both the *adoption* and *implementation* of the protocol over time, and demonstrate how its utilization altered patterns of social interaction in ways that would not have happened if some other standard (or no standard) had been adopted. Isolating these effects from all the other things affecting the trajectory of society isn't easy.

To recognize that a protocol influences political or social outcomes is not the same as saying that the protocol itself "has" politics or "embeds" a specific politics. To begin with, if a standard is not adopted then it cannot have any effects; agency regarding adoption resides in the organization or person, not in the standard itself. Implementation decisions are another shaping variable. Standards often enable their users to choose implementations that reflect their own preferences. While the standard limits options and enables/disables certain things, a great deal of agency still resides in the implementer. One can, for example, implement BGP routing protocols to block all IP addresses known to be associated with web sites with certain religious content. The protocol allows but doesn't dictate this politically salient choice. Furthermore, not all of the affordances can be predicted by the developers of the standard; they may be unintentional or emergent. [3] The SES approach allows for substantial divergence between the intentions of protocol designers and the social effects of its adoption and use. So a standard's societal impact cannot be known *a priori* merely by specifying it; in this sense it is misleading to say that a particular societal shaping is "embedded" or "baked" into the design. And even when influence occurs, the impact of most protocols is likely to be narrowly confined to one component of a particular technical system; it would be rare for a single protocol to have a major societal impact by itself. Hundreds of other factors (e.g., wars or depressions, market structure, business strategies, government regulations, path dependency) will be involved.

3: Protocols have politics (PHP)

A third position asserts that protocols *have politics.* That is, a certain power relations are embodied in the standard/protocol itself, such that anyone who uses it deterministically reflects or reproduces these relations. The PHP position is expressed well by ten Oever and Cath's call for "hard-coding human rights into protocols" because "design choices have offline consequences and are able to shape the power positions of groups or individuals in society." [2] It was also present in a major National Science Foundation project for the development of a future Internet which stated, "if we accept that architecture, protocol, and mechanisms can embody values, let those who design and produce systems take into consideration, that is, engineer, values as among the functionalities and constraints of their systems." [20] This view has achieved the status of a kind of folk wisdom, as exemplified by a statement from a U.S. State Department official that "The positive values that [civil society] supports and believes in are engineered right into the logic of the Internet's protocols."[3] Note that

[3] Stephen Anderson, Acting Deputy Assistant Secretary for International Communications and Information Policy, Transcript of UN Internet Governance Forum Workshop #81, "Overcoming the US-China Digital Cold War," November 10, 2020.

PHP and SES both address the potential *effects* of technology, but PHP focuses attention upon the intrinsic features of the protocol or technology design itself, not the adoption and implementation decisions made by people and organizations. It asserts that the societal effects are directly caused by the design choices that enable certain capabilities and not others. Different ways of implementing the protocol are not explicitly recognized as a relevant factor, and the ability to refuse to adopt a protocol or technology is not taken into account.

This third, stronger position must be recognized as a variant of technological determinism. It bears important similarities to the "technology constructs society" view advanced by Langdon Winner [21] [22] and philosopher Jacques Ellul [23]. Those theorists, however, focused on the societal imperatives generated by large-scale technological systems rather than on specific protocols/standards. PHP constitutes an oddly micro-level version of technological determinism. But it is more likely that PHP got its inspiration from Lawrence Lessig's famous "code is law" thesis [24]. Much of Lessig's rhetoric could be interpreted as a PHP variant, such as his statement "We can build, or architect, or code cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear." [25] Agency is located in intentional design. Lessig was not as specific as the PHP advocates about where this building, architecting or coding took place, though. His examples of how "code" governs behavior almost always refer to the implementation choices of system operators rather than to protocol design.

To conclude this section, three distinct meanings or interpretations of how protocols or standards might shape society or be political have been described. The utility and applicability of all three of these meanings can be put to the test by examining the actual development, implementation and use of a new protocol, TLS 1.3. TLS 1.3 was intentionally created to support privacy and cybersecurity, which are critical values and policy objectives in contemporary Internet governance. The rest of the paper examines the development of TLS 1.3.

THE SNOWDEN REVELATIONS

TLS 1.3 is best understood as a wholesale revision of prior versions of TLS (particularly TLS 1.2, documented in RFC 5246, August 2008) after the June 2013 Edward Snowden leaks. Snowden disclosed troves of data about the US National Security Agency's (NSA) surveillance programs. [26] Journalistic reports about Snowden's revelations insinuated that internet service providers and technology companies were complicit in providing the intelligence community with the access necessary to engage in mass surveillance. [27]

Another damaging claim by Snowden was his confirmation that in 2004 the NSA paid RSA Security to implement a cryptographically weak pseudorandom number generator known as a CSPRNG. CSPRNGs are instrumental in generating viable cryptographic keys. The CSPRNG commissioned by the NSA and included in RSA's BSAFE cryptographic library was called the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG). Dual_EC_DRBG was then published by NIST in Special Publication 800-90A, Rev. 1 *Recommendation for Random Number Generation Using Deterministic Random Bit Generators* - despite a mathematical demonstration of the potential for a trapdoor. [28] Perhaps the most damaging documents released were those suggesting that the NSA had exploited Internet infrastructure for indications and warnings of opposition-force computer network attacks, and for enabling man-in-the-middle injection attacks. [29] [30]

To illustrate the broader effect of Snowden's initial releases, the leaders of the Internet technical community and several US government agencies underwent a series of major shifts in response to the exposure of American surveillance activities. These responses were designed to restore trust in the global Internet infrastructure:

1. October 2013 - A joint statement by leaders of the Internet technical community (the IETF's Internet

Architecture Board, the Internet Corporation for Assigned Names and Numbers, the regional Internet address registries, and the WorldWide Web Consortium) "expressed strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance." They called upon the U.S. government to "accelerat[e] the globalization of ICANN and IANA functions."[4]

2. March 2014 - the US Commerce Department's National Telecommunications and Information Administration (NTIA) announced that it would facilitate the transition of the IANA functions to the private sector.[5]
3. April 2014 - NIST removed the now-suspect RC4 and Dual_EC_DRBG cryptographic algorithms from its published guidance in NIST Special Publication 800-90A, Rev. 1).
4. April 2014 - the IETF announced work on TLS 1.3
5. May 2014 - the IETF released a document that defined pervasive monitoring as "a technical attack that should be mitigated in the design of IETF protocols." [31]
6. February 2015 - NIST reformed its process for developing and managing cryptographic standards.[6]

It is impossible to see the development of TLS 1.3 as anything but a response to the politics of surveillance on the part of the Internet's leading SDO and many others involved in Internet governance.

PERFECT FORWARD SECRECY: THE TLS 1.3 STANDARD

The Transport Layer Security (TLS) 1.3 protocol seeks to make pervasive surveillance more difficult by removing Rivest-Shamir-Adleman (RSA) key exchange, with its static private keys, in favor of Diffie-Hellman (DH) key exchange and mandatory Perfect Forward Secrecy. [32] Perfect Forward Secrecy (PFS) is a cryptographic technique that replaces static private keys with session-specific ephemeral keys, removing the possibility of decryption of internet traffic at scale if a single key is compromised. Thus, in theory, if widely implemented PFS makes mass surveillance more difficult.

The IETF decided to adopt DH key exchange because the documents made available by Snowden suggested that the NSA and its Five Eyes partners engage in both "upstream" and "downstream" collection efforts that violate security and privacy principles with the explicit cooperation of industry. In the US, this includes the use of Foreign Intelligence and Surveillance Act (FISA) warrants executed through Title 18 authorities, and expanded powers under the USA PATRIOT Act. Both can be used to compel companies to hand over bulk data ("downstream") and to gain access to internet backbone providers and telecommunication companies ("upstream") in order to put in place surveillance implants, including subversion of cryptographic standards and other schemes for surreptitious decryption of internet traffic. Thus the requirement for PFS became a driving

[4] Montevideo Statement on the Future of Internet Cooperation, Uruguay, 7 October 2013. Retrieved from https://www.arin.net/vault/about_us/media/releases/20131007.html. The IANA functions refer to the centralized coordination of the Internet's naming, numbering and protocol parameter values. At that time the IANA functions were delegated to ICANN by means of a contract with the U.S. Commerce Department. "Globalization of the IANA functions" was a commonly-used expression within the ICANN regime meaning ending of U.S. government control of the functions.
[5] NTIA Announces Intent to Transition Key Internet Domain Name Functions, March 14, 2014, https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions
[6] NIST Cryptographic Standards and Guidelines: A Report to the NIST Visiting Committee on Advanced Technology Regarding Recommendations to Improve NIST's Approach. February 2015. https://www.nist.gov/system/files/documents/2017/05/09/Report-to-VCAT-and-COV-Feb-2015.pdf

force in creating TLS 1.3. It was seen as a way to address these “attack vectors” by removing the possibility for both passive and active decryption through the compromise of a single key.

To fully understand the political economy of the standardization process, one must examine the specific people and organizations involved in the construction of the protocol, as participants may have brought along the agendas of their respective organizations. The group’s original charter designated Christopher Wood, Joseph Salowey, and Sean Turner as working group chairs. Christopher Wood is a relatively young computer scientist who completed his Ph.D. in 2017 at the University of California at Irvine while co-chairing the IETF TLS Working Group. Concurrent to this period Wood also worked at the Palo Alto Research Center, a major partner in federally funded government research. Joseph “Joe” Salowey has industry experience at Cisco Systems, F5 Networks, and Tableau Software and has been involved in IETF working groups for more than a decade. Sean Turner graduated from Georgia Tech in 1993 and has remained an independent consultant serving in various capacities at the IETF and the Internet Society for close to two decades.

In addition to the Working Group members listed above, regular contributors included individuals from across the industry who interfaced with IETF engineers online and at various conferences held throughout the four years of the protocol’s development. The stakeholders involved in the creation of TLS 1.3 in the IETF TLS Working Group included Content Delivery Network (CDN) providers Akamai [33] and Cloudflare [34], British security firm NCC Group [35], and other technical experts from across the industry. Working Group Chair Sean Turner noted that both ACLU advocates and NSA representatives were present at several conferences to provide their perspectives on the development of the protocol. [36] Finally, Google and Facebook were active in early-stage development, rolling out related products "BoringSSL” and “Fizz” [33], with the former inspiring further work on QUIC-over-HTTP or HTTP/3.

Aside from PFS, the new TLS standard touts performance improvements as another benefit. (Fig. 1) These performance improvements include a reduction in the number of steps in the TLS handshake by using a Diffie-Hellman schema and the introduction of support for Zero Round Trip Time (0-RTT) responses for the resumption of cached sessions. A related development is that TLS 1.3 can be an ancillary technology for securing the “Quick UDP Internet Connections” (QUIC) protocol. Originally developed at Google, QUIC allows for multiplexing and encryption of UDP-based datagrams, which are used in streaming services such as voice calls or video transmissions. This allows streaming data to be sent confidentially over the public Internet instead of just on private circuits. Previously, security concerns often required provisioning of dedicated lines for multicast. QUIC is also the basis of the new proposed HTTP/3 standard, which is still in development at the IETF.

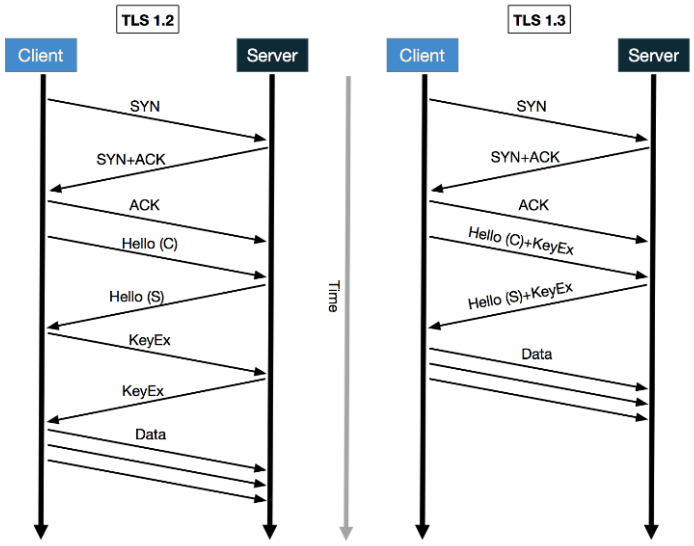


Figure 1: TLS Handshake Comparison

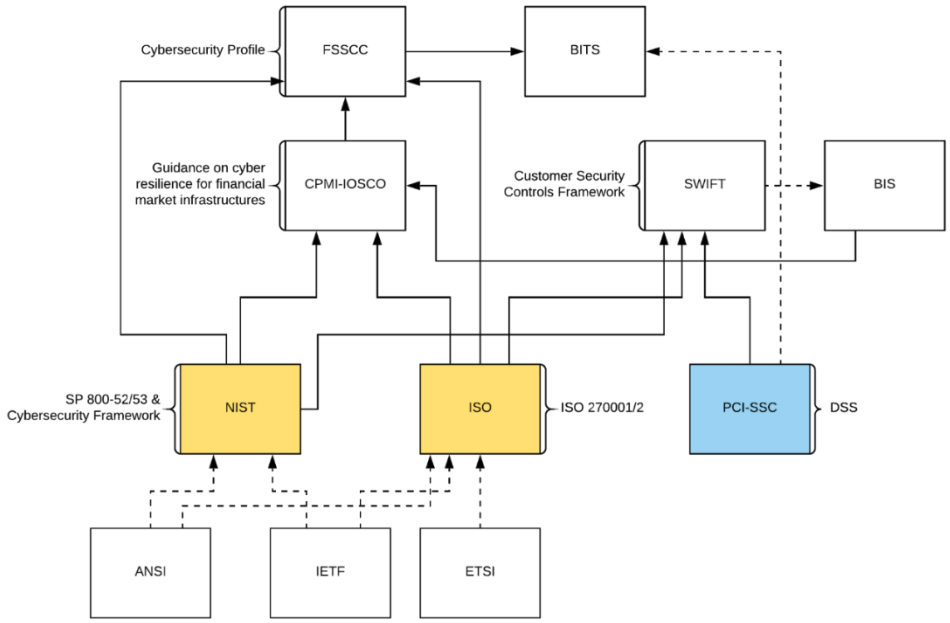
HTTP/3 incorporates the TLS 1.3 handshake and at the transport layer uses QUIC streams designed on top of UDP instead of TCP for better performance, security, and reliability over previous versions. Thus, TLS 1.3 is more than just a confidentiality improvement on TLS 1.2; it is an integral security component of the next generation of Internet protocols and technologies.

DISSENSION OVER THE STANDARD

PFS was an improvement for those seeking to advance the confidentiality of data on the internet, but it also had its detractors. Those opposed to mandated PFS were concerned with its implications for the use of various Deep Packet Inspection (DPI) technologies. DPI technologies include both inline middleboxes like firewalls and intrusion detection systems, and out-of-band devices or "taps." Both rely upon private key stores in order to decrypt TLS traffic for internal network troubleshooting and security analysis.

The development of TLS 1.3 gave rise to a contest between privacy proponents at IETF and representatives of the banking industry. On 22 September 2016, Andrew Kennedy of the Bank Policy Institute (BPI) first raised an objection in an email to the IETF TLS Working Group stating: "While I am aware and on the whole supportive of the significant contributions to Internet security this important working group has made in the last few years I recently learned of a proposed change that would affect many of my organization's member institutions: the deprecation of RSA key exchange."[7] In the message, he further detailed the complications that the removal of static private RSA keys would cause due to his members' need for "out-of-band TLS decryption." Kennedy's complaint centered on the IETF's preference for Diffie-Hellman key exchange over the traditional RSA key exchange, and the fact that PFS was *required* in TLS 1.3, whereas in TLS 1.2, PFS was an optional feature.

Figure 2 below is a diagram of the relationships among agencies and organizations with a stake in financial security standards. The division of the Bank Policy Institute for which Andrew Kennedy spoke is the Business Innovation Technology and Security division (BITS). BITS relies upon a cybersecurity framework published by the Financial Services Sector Coordinating Council (FSSCC). The framework is described as a Financial Services Sector Cybersecurity Profile, which in turn draws on standards published by NIST and the International Standards Organization (ISO). They map their "Profile" to the "ISO 27000 series of controls [and] CPMI-IOSCO's 'Guidance on cyber resilience for financial market structures.'" ("Financial Services Sector Cybersecurity Profile," n.d.) CPMI-IOSCO refers to the Committee on Payments and Market Infrastructures of the International Organization of Securities Commissions. CPMI-IOSCO draws on NIST documentation, is endorsed by the Bank for International Settlements (BIS), and orchestrates "…the safety and efficiency of payment, clearing, settlement, and related arrangements, thereby supporting financial stability and the wider economy." (CPMI-IOSCO)



[7] "Industry Concerns about TLS 1.3," Email from Andrew Kennedy, BPI, to TLS Working Group, 22 September 2016. https://mailarchive.ietf.org/arch/msg/tls/KQIyNhPk8K6jOoe2ScdPZ8E08RE/

Figure 2: Security Standards Ecosystem

Not specifically within the FSSCC's guidelines, but tangentially related, is the Payment Card Industry Security Standards Council (PCI-SSC), whose membership includes Visa, American Express, Discover and several other financial sector participants. The FSSCC does not specify a specific TLS protocol for end-to-end encryption, although NIST Special Publication 800-52, which the FSSCC draws upon, does. The PCI-SSC also specifies encryption protocols under guidelines published in their "Data Security Standards" (DSS). In June 2018, the PCI-DSS mandated that any transmission of payment card information must be encrypted with TLS 1.2. [37] This specification also influences global payments transfer through the Society for Worldwide Interbank Financial Telecommunications (SWIFT) Customer Security Programme. SWIFT also requires TLS 1.2, as it draws source material from NIST, ISO 27002, and the PCI-DSS. [38] This means that if NIST, ISO, or even the PCI SSC formally recommended implementation of TLS 1.3, then BITS might also be forced to advise its members to do so.

So why did BITS resist PFS and TLS 1.3? It was concerned with both cost and security issues. A PFS mandate would undercut their ability to engage in out-of-band TLS decryption using DPI technologies that are already widely deployed in their networks. Inline and out-of-band DPI provides an economical way of monitoring traffic within a large enterprise infrastructure. A move to ephemeral keys with TLS 1.3 would impair their ability to monitor internal traffic unless they made expensive infrastructure investments in endpoint monitoring solutions or in novel ephemeral key store technology, potentially leaving stranded capital in legacy DPI appliances. The BITS group justified their interest in out-of-band decryption with their own interest in cybersecurity. The security of their private networks, in their view, required greater visibility into what was happening on their systems. TLS 1.3 provides stronger security for end-users, but reduce**s** enterprise network managers' visibility into what is going on inside their own networks without significant investment in new infrastructure.

BITS' concerns about enterprise network visibility stemmed in part from their regulatory obligations. Hence, it is important to understand the laws that govern their business operations. The Sarbanes-Oxley (SOX) Act of 2002 mandates internal controls that allow for compliance monitoring, and has been interpreted to be a critical priority for IT security managers in the financial sector. SOX was enacted after several corporate scandals at Enron, Tyco, and WorldCom. SOX Section 404 is particularly pertinent as it requires the ability for a full audit. Compliance is typically managed using several different frameworks, including ISO 17799, the Information Systems Audit and Control Association's Control Objectives for Information and Related Technologies (COBIT), and the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control – Integrated Framework. In addition to Section 404 compliance, the financial sector must comply with the Securities Exchange Act of 1934 to prevent insider trading, the 1970 Bank Secrecy Act to prevent money laundering, and the 2001 USA PATRIOT Act to detect terrorist financing -- all of which might encourage a financial services enterprise to retain the capability for out-of-band decryption as an economical means of complying with these laws.

Even if the companies in BITS adopted TLS 1.3, however, it would not completely prevent them from engaging in the security and surveillance activities necessary to protect their infrastructure and ensure compliance with the law. Enterprises can use Security Information and Event Management (SIEM) platforms, coupled with logging and monitoring agents on endpoints, to accomplish what they did previously with DPI solutions like NetScout. However, system and network troubleshooting does become more problematic, considering the complexity of enterprise network architectures. There are solutions such as ExtraHop's Decryption Suite which has tackled the problem of out-of-band TLS decryption even with perfect forward secrecy. This is accomplished by an agent forwarding ephemeral keys to an appliance that can call up recorded sessions for investigation and decrypt those using keys correlated to net flows advertised by IP headers and timing. While the computational load for this technology carries significant overhead (particularly for real-time decryption), if architected

correctly an ephemeral key store should be out-of-band and thus less disruptive, making BITS' arguments on these grounds perhaps unwarranted other than to acknowledge increased complexity and cost.

Mr. Kennedy of BITS also expressed concerns that with TLS 1.3 "enterprises who use content delivery networks will have the end-user session hidden from them." That is a valid point with broader implications than just an enterprise attempting to monitor its traffic. A great amount of trust must be given to any content delivery network (CDN) provider which is not organic to an organization or group. At the edge, a CDN acts as its own DNS forwarder and/or resolver, in some cases providing little visibility as to where packets have hopped, especially with TLS being renegotiated from the edges of the CDN to the distant server. This can eliminate client-server visibility completely. Should the CDN itself be compromised or complicit in surveillance, it could also allow for Man-in-the-Middle attacks like those which Snowden disclosed in 2013. This is not a problem unique to TLS 1.3, but TLS 1.3 does increase the difficulty of tracking sessions across the CDN. Technical solutions are available for this problem as well, but they are not cheap.

Opposition to mandatory PFS in the standard eventually gave rise to a unique situation: After the IETF refused to incorporate static keys in the protocol, U.S. government agencies and American private corporations turned to a competing, European standards body to develop an alternative. In early 2017 some vendors and user groups turned to the Technical Committee on Cybersecurity (TC CYBER) of the European Telecommunications Standards Institute (ETSI). ETSI's TC CYBER eventually produced a competing protocol known variously as Enterprise Transport Security (ETS), Middlebox Security Protocol, or Enterprise TLS. [39] It remains to be seen if the banking industry will adopt ETSI's alternative transport security standard, but an entry has already been recorded in the NIST National Vulnerability Database (NVD) regarding its lack of Perfect Forward Secrecy.[8]

Not surprisingly, BITS has worked to prevent NIST from issuing a recommendation to implement TLS 1.3. In "Public Comments on the Second Draft of NIST Special Publication 800-52 Revision 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (October 15, 2018)", SAIC and Verisign alumni Anthony M. Rutkowski of ETSI's cyber security working group, stated that NIST should consider "…the significant harms potentially resulting from NIST proposed TLS 1.3 implementations." Rutkowski cited TC CYBER's work with Microsoft, middlebox producer NetScout, various US national security entities, U.S. Bank, and researchers at Johns Hopkins University in vetting the proposed ETS encryption protocol. NIST SP 800-52 suggested a TLS 1.3 implementation date of 2024, leaving it open for ETSI and groups like BITS to implement the ETS protocol, which by their own specification can subvert TLS 1.3 clients by rendering them "...unaware that eTLS (ETS) and therefore static Diffie-Hellman is in use, as it is not given the information...." If ETS can be used to surreptitiously maintain a private key when it interacts with TLS 1.3 clients, pervasive and covert monitoring is still a capability despite the efforts of the IETF WG.

It should be noted that ETS is designed to be compatible with unmodified TLS 1.3 clients. Connecting TLS 1.3 clients that are modified for ETS can allow for extensions that negotiate a specific ETS handshake, which includes an "awareness" feature announcing middleboxes on the wire. This notification could advance privacy only insofar as it allows the connecting client to drop the session. ETS uses a Diffie-Hellman key exchange, but instead of truly ephemeral keys, it allows the enterprise to rotate static Diffie-Hellman keys instead of generating unique keys for every session as with true PFS. The Electronic Frontiers Foundation, a privacy advocacy organization, has opposed the use of this "complementary" protocol because of its lack of true PFS. [39]

CONCLUSION: TLS 1.3 AND POLITICS IN PROTOCOL DESIGN

[8] NIST National Vulnerability Database, CVE-2019-9191. https://nvd.nist.gov/vuln/detail/CVE-2019-9191

The story of TLS 1.3 leads to a number of interesting observations about the role of politics in protocols. One thing is clear: it was certainly the *intention* of the designers of TLS 1.3 to advance privacy protection. And insofar as the standard is adopted and implemented *as intended*, it does indeed strengthen the confidentiality of internet communications relative to its predecessors. Certificate exchange is now encrypted in the TLS 1.3 handshake. This improves previous versions, where ServerHello messages and certificates were transmitted in the clear, announcing the destination hosts that the client is attempting to reach. Extensions to encrypt Server Name Indication (SNI) are also incorporated into TLS 1.3, further protecting the privacy of DNS queries when combined with DNS over HTTPS (DoH).

But it is equally clear from this narrative that it would be a mistake to assign primacy to the protocol design in governing privacy and security on the internet. The protocol's features were but one component of a much wider politics and economics around privacy and surveillance. In this contest, human actors and the organizations in which they were situated used various tools to advance their goals. The protocol design in IETF was only one of many avenues available to shape the overall status of privacy and surveillance. It is also noteworthy that many of the opponents of TLS 1.3's use of PFS were supportive of the same value – cybersecurity – but believed that the lack of internal visibility created by TLS 1.3 undermined the security of their own local situation. As a summary, it is useful to look at each of the three positions outlined in our framework and see how the evidence from this case study relates to it.

PES: Stakeholder interests drive design

TLS 1.3's development narrative shows interest groups contending over the design. Conflict centers on whether there should be a PFS mandate or not. Privacy advocates, civil libertarians and big tech firms who felt burned by NSA surveillance tended to support PFS while representatives of the banking sector, large enterprise networks and some advocates associated with government agencies opposed it. It was the political views of the people who pushed for stronger encryption that shaped the protocol, not the other way around. While the advocates of a PFS mandate won in the IETF, an SDO with a long history of support for privacy rights on the Internet, that victory merely led opposing stakeholders to develop a competing standard in another SDO, ETSI, where the political and economic views of a different set of stakeholders prevailed. (The prospect of a fork in development led to interesting debates within the IETF about whether it was better to compromise and adjust the standard to accommodate its critics so as to support compatibility and keep the disaffected parties within the confines of the IETF [40].)

Note also that opposition to PFS was driven more by business concerns and different perspectives on cybersecurity, than by a competition over political power. Critics of TLS 1.3 had an interest in retaining visibility into their own network traffic for purposes of their own security and regulatory compliance. They also wanted to salvage the value of their DPI middleboxes and avoid the added expense of deploying the new technologies needed to achieve such visibility in the context of PFS.

SES: Societal effects unclear.

The fact that PFS was built into the protocol constituted a victory for the privacy advocates, but by no means did it "bake" values into the internet, much less into society as a whole. Understanding societal effects, as noted in the conceptual framework, requires monitoring both adoption decisions and the aggregate effects of various implementations of the standard. Regarding adoption, the IETF is the authoritative SDO for most Internet protocols, but adoption of its standards is entirely voluntary. Adoption decisions are mediated by the political and economic incentives of a diverse set of stakeholders, some of whom did not favor PFS. Consequently there were efforts to delay endorsements of TLS 1.3 within security standards organizations in order to retard adoption. Slowing down adoption would attenuate the costs incurred by PFS opponents. A

competing standard (ETS) was also developed that is compatible with TLS 1.3 but can be used to undermine PFS.

Statistics regarding adoption show that the proportion of TLS 1.3 users increased steadily from 2018 to the end of 2019, but its security enhancements have not yet triggered wholesale conversion to the new standard. Observations of actual adoption and use at the end of 2019 show that 17% of the Alexa Top 100,000 websites supported TLS 1.3 while about 60% supported TLS 1.2 and just under 23% were using even older, less secure protocols. [41] [42] The substantial chunk of users relying on older protocols is not just a statement about political values, but a testimony to the power of inertia as well.

An unexpected, non-political factor may drive more rapid adoption of TLS 1.3, however: marketplace demand for better performing web services. Gaming platforms such as Google's cloud-based streaming 'Stadia' could benefit greatly from the lower-latency encryption found in ancillary technologies like QUIC. TLS 1.3 is required to encrypt QUIC; in turn, QUIC is required for the next generation of HTTP protocol (HTTP/3). In other words, the TLS 1.3 protocol's enhanced technical efficiency, and its compatibility with other new protocols might play a critical role in incentivizing its adoption. This use case for TLS 1.3 is a far cry from what privacy and human rights advocates have advertised. The view that "protocols have politics" tends to think only of intentional effects and discount or overlook politically neutral drivers of adoption such as technical efficiency and compatibility with other protocols. Indeed, these critics sometimes even ridicule statements by protocol designers that they are interested in addressing such "purely technical" problems.

Regarding implementation, we showed that new technical solutions are being developed that allow some of the privacy-enhancing features of PFS to be undermined. While they are expensive now, their cost may decline over time, and other workarounds may be developed. It is also possible to achieve privacy improvements such as PFS and deprecation of weak ciphers with extensions to TLS 1.2. [43]

Looking to the broader social environment, TLS 1.3's implementation process occurs as the U.S. government continues to attack "warrant-proof encryption"[9] and certain elements of the national security establishment have demonstrated a long-term interest in legislative or policy actions that will reduce or compromise the ability of the private sector to implement end to end encryption.[10] Outside the U.S., many governments already restrict encryption in various ways and/or block applications and services that deploy end to end encryption. In August 2020, news reports surfaced that the government of China was blocking all web connections using TLS 1.3. [44] This was done to prevent Encrypted Server Name Indication, a key security feature of the standard, from obscuring the domain being access from censors. Given these actions, it is an obvious mistake to see a direct relationship between protocol design and societal effects. There are many other shaping factors. All these caveats show that it is too early to know how much the new standard will curb state surveillance or contribute to overall societal privacy. TLS 1.3 is more accurately described as an unevenly distributed escalation of the technical difficulty needed to surveill, rather than as a protocol that "hard codes" privacy rights into the Internet.

PHP: Protocols as politics by other means

As for the third approach, the insertion of PFS into the new protocol as a default did promote the value of confidentiality by giving collective approval to a technical design that was more secure than its predecessor. But we have shown how barriers to its adoption were deliberately raised by some stakeholders, and we have seen

[9] Attorney General William P. Barr Delivers Remarks at the Lawful Access Summit Washington, DC. October 4, 2019. https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-lawful-access-summit

[10] S.4051 - Lawful Access to Encrypted Data Act 116th Congress (2019-2020). https://www.congress.gov/bill/116th-congress/senate-bill/4051/

how future implementations or the choice of an alternate standard can shape overall societal effects as much as the use of TLS 1.3. We have also indicated broader legislative and policy currents that undermine encryption and privacy.

The Internet Research Task Force's (IRTF) statement on "Human Rights Protocol Considerations" (HRPC) approvingly quotes a statement from Janet Abbate's book *Inventing the Internet* that "protocols are politics by other means." The RFC authors interpret Abbate's statement as meaning that "the values and ideas about the role that a particular technology should perform in society are embedded into the design." What the authors may have missed is that Abbate's statement is likely a reference to Carl von Clausewitz's 1832 work *On War* where he famously stated, "War is the continuation of politics by other means." If the double entendre was intended, Abbate's statement takes on a meaning that diverges from the interpretation of PHP, and is more in line with PES. A better interpretation would be that the process of standardizing and implementing TLS 1.3 reflects conflicting values, ideas and economic interests among different groups. The formal specification of the standard is but one tactic or tool in their struggle. It does not inscribe values onto a technical system in a way that automatically realizes them in society. The values and politics are not "in" the protocol per se but in the surrounding actors, who utilize the protocol and many other devices (SDOs, the recommendations of industry and regulatory bodies, law, and competing technologies, to name a few) to push for their goals. Those goals are often monetary and market-driven, not just political in the narrow sense. In the development of TLS we see a war of ideas and interests fought in part through protocol design decisions, but also by adoption and implementation decisions, by new technologies and workarounds, and in legislation and public policy. In the IETF, privacy advocates won a battle, but not the war.

To conclude, the relationship between technology and society has been a notoriously complex and slippery area of scholarship for decades. This case study shows that the successful standardization of a security protocol does have some efficacy as a means of shaping the playing field. But a clearer and more differentiated understanding of the relationship between standards, standardization processes, adoption and implementation is needed if an accurate assessment of societal impact is to be made. Our conceptual framework clarified three distinct ways in which politics, interests and standards might intersect. Ultimately it is humans, not protocols, that have politics, values and economic interests, and it is human interaction with standards and technical systems that drive societal effects.

GLOSSARY OF TERMS

ACLU - American Civil Liberties Union

BIS - Bank for International Settlements

BITS - Business Innovation Technology and Security (BPI)

BPI - Bank Policy Institute

CDN - Content Delivery Network

CNA - Computer Network Attacks

COBIT - Control Objectives for Information and Related Technologies (ISACA)

COSO - Committee of Sponsoring Organizations of the Treadway Commission

CPMI - Committee on Payments and Market Infrastructures (IOCSO)

CRFG - Crypto Forum Research Group

DPI - Deep Packet Inspection

EFF - Electronic Frontiers Foundation

eTLS - Enterprise TLS (ETSI)

ETS - Enterprise Transport Security (ETSI)

ETSI - European Telecommunications Standards Institute

FSSCC - Financial Services Sector Coordinating Council

GCHQ - Government Communications Headquarters (UK)

HRPC RG - Human Rights Protocol Considerations Research Group

IANA - Internet Assigned Numbers Authority

ICANN - Internet Corporation for Assigned Names and Numbers

IETF - Internet Engineering Task Force

IOCSO - International Organization of Securities Commissions

IP - Internet Protocol

IRTF - Internet Research Task Force

ISACA - Information Systems Audit and Control Association (ISACA)

ISO - International Standards Organization

MSP - Middlebox Security Protocol

NIST - National Institute of Standards and Technology

NSA - National Security Agency (US)

NTIA - National Telecommunications and Information Administration

NVD - National Vulnerability Database (NIST)

PCI-DSS - Payment Card Industry Data Security Standards (PCI-SSC)

PCI-SSC - Payment Card Industry Security Standards Council

PFS - Perfect Forward Secrecy

QUIC - Quick UDP Internet Connections

RFC - Request for Comments (IETF)

SOX - Sarbanes-Oxley Act of 2002

SWIFT - Society for Worldwide Interbank Financial Telecommunication

TC CYBER - Technical Committee on Cybersecurity (ETSI)

TLS - Transport Layer Security

0-RTT - Zero Roundtrip

REFERENCES

[1] E. Rescorla, "RFC 8446, Transport Layer Security (TLS) Protocol Version 1.3," Internet Engineering Task Force (IETF), August 2018.

[2] N. ten Oever and C. Cath, "RFC 8280 Research into Human Rights Protocol Considerations," Internet Research Task Force (IRTF), October 2017.

[3] M. L. Mueller and F. Badiei, "Requiem for a dream: On advancing human rights via internet architecture," *Policy & Internet,* vol. 11, no. 1, pp. 61-83, 2019.

[4] C. Cath and L. Floridi, "The design of the internet's architecture by the Internet Engineering Task Force (IETF) and human rights," *Science and Engineering Ethics,* vol. 23, no. 2, pp. 449-68, 2017.

[5] L. DeNardis, Protocol politics: The globalization of Internet governance, Cambridge, Mass: MIT Press, 2009.

[6] J. Abbate, Inventing the internet, Cambridge, Mass: MIT Press, 2000.

[7] C. Knobel and G. Bowker., "Values in Design," *Communications of the ACM,* vol. 54, no. 7, pp. 26-28, 2011.

[8] H. Nissenbaum, "How Computer Systems Embody Values," *Computer,* vol. 34, no. 3, pp. 118-120, 2001.

[9] I. Rubinstein, "Regulating Privacy by Design," *Berkeley Technology Law Journal,* vol. 26, no. 3, p. 1409–56, 2011.

[10] M. Flanagan, D. Howe and N. Nissenbaum, "Embodying Values in Technology: Theory and Practice," in *Information Technology and Moral Philosophy, eds. J. van den Hoven and J. Weckert*, Cambridge, Cambridge University Press, 2008.

[11] M. L. Mueller, Networks and states: The global politics of Internet governance, Cambridge, Mass: MIT Press, 2010.

[12] D. D. Clark, Designing an Internet, Cambridge, Mass: MIT Press, 2018.

[13] I. Brown, Research Handbook on Governance of the Internet, Cheltenham: Edward Elgar Publishing Ltd, 2013.

[14] J. K. Knight, Institutions and social conflict, Cambridge, UK: Cambridge University Press, 1992.

[15] R. Crane, "Communication standards and the politics of protectionism: The case of colour television systems," *Telecommunications Policy,* vol. 2, no. 4, pp. 267-81, 1978.

[16] J. Hart, "The politics of HDTV in the United States," *Policy Studies Journal,* vol. 22, no. 2, pp. 213-28, 1994.

[17] W. Mattli, "The politics and economics of international institutional standards setting: an

introduction.," *Journal of European Public Policy,* vol. 8, no. 3, pp. 328-44, 2001.

[18] I. Hutchby, "Technologies, texts and affordances," *Sociology,* vol. 35, no. 2, pp. 441-56, 2001.

[19] C. Shapiro and H. R. Varian, Information rules: a strategic guide to the network economy, Cambridge, Mass: Harvard Business Press, 1998.

[20] H. Nissenbaum, "Values in Design Council: An End of Project Report," NSF EAGER, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.386.5320&rep=rep1&type=pdf, 2013.

[21] L. Winner, Autonomous technology: Technics-out-of-control as a theme in political thought, Cambridge, Mass: MIT Press, 1978.

[22] L. Winner, "Do artifacts have politics?," *Daedalus ,* pp. 121-136, 1980.

[23] J. Ellul, The Technological Society, New York: Vintage (English translation), 1954.

[24] L. Lessig, Code and Other Laws of Cyberspace, New York: Basic Books, 1999.

[25] L. Lessig, Code, New York: Perseus Group, 2006.

[26] A. Wills, "New Snowden leak: NSA program taps all you do online," *CNN Online,* 31 July 2013.

[27] S. Ackerman, "US tech giants knew of NSA data collection, agency's top lawyer insists," *The Guardian,* pp. https://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de , 19 March 2014.

[28] M. Wertheimer, "The Mathematics Community and the NSA," *Notices of the AMS,* pp. http://www.ams.org//notices/201502/rnoti-p165.pdf, February 2015.

[29] B. Schneier, "How the NSA Attacks Tor/Firefox Users," *Schneier on Security,* p. https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html , 7 October 2013.

[30] N. Weaver, "A Close Look at the NSA's Most Powerful Internet Attack Tool," *Wired,* p. https://www.wired.com/2014/03/quantum/, 13 March 2014.

[31] S. Farrell and H. Tschofenig, "RFC 7258: Pervasive Monitoring Is an Attack," Internet Engineering Task Force (IETF), https://tools.ietf.org/html/rfc7258, May 2014.

[32] J. Leyden, "Net tech bods at IETF mull anti-NSA crypto-key swaps in future SSL," *The Guardian,* 8 May 2014.

[33] R. Salz, "TLS 1.3 FTW," *The Akamai Blog,* pp. https://blogs.akamai.com/2017/01/tls-13-ftw.html, 25 January 2017.

[34] N. Sullivan, "Introducing TLS 1.3," *Cloudflare Blog ,* pp. https://blog.cloudflare.com/introducing-tls-1-3/, 20 September 2016.

[35] S. Stender, "NCC Group's Cryptography Services audits our Go TLS 1.3 stack," *Cloudflare Blog ,* pp. https://blog.cloudflare.com/ncc-groups-cryptography-services-audit-of-tls-1-3/, 15 February 2017.

[36] D. Coldewey, "The messy, musical process behind the web's new security standard," *Tech Crunch,* pp. https://techcrunch.com/2018/06/11/the-messy-musical-process-behind-the-webs-new-security-standard/, 11 June 2018.

[37] L. Gray, "Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS," *PCI Security Standards Council Blog,* pp. https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls, 30 June 2017.

[38] S. Gilderdale and T. Wicks, "SWIFT's Customer Security Programme (CSP) is well underway. What has it achieved to date, and what are the next key milestones?," SWIFT, https://www.swift.com/news-events/news/swift_s-customer-security-programme-csp_is-well-underway_wh, June 12 2017.

[39] J. Hoffman-Andrews, "ETS Isn't TLS and You Shouldn't Use It," Electronic Frontiers Foundation, San Francisco, 26 February 2019.

[40] S. Checkoway, "TLS 1.3 in Enterprise Networks," *Blog post,* pp. https://checkoway.net/musings/tls13-enterprises/, 22 July 2017.

[41] P. Nohe and D. Beatty, "The CA Security Council Looks Ahead to 2020 and Beyond," *CA Security Council blog,* pp. https://casecurity.org/2020/01/09/the-ca-security-council-looks-ahead-to-2020-and-beyond/, 9 January 2020.

[42] B. Weber, "Benefits and Adoption Rate ofTLS 1.3," SANS Institute, https://www.sans.org/reading-room/whitepapers/vpns/benefits-adoption-rate-tls-13-39715, August 2020.

[43] D. Holmes, "The 2017 TLS Telemetry Report," F5 Labs, https://www.f5.com/content/dam/f5/f5-labs/articles/20180423_tls_2017/2017_TLS_Telemetry_Report.pdf, April 2018.

[44] C. Cimpanu, "China is now blocking all encrypted HTTPS traffic that uses TLS 1.3 and ESNI," *ZDNet,* pp. https://www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/, 8 August 2020.