Harvard Journal of Law & Technology
Volume 30, Number 2 Spring 2017

ENCRYPTION$^{\text{CONGRESS}}$ MOD (APPLE + CALEA)

*Justin (Gus) Hurwitz**

TABLE OF CONTENTS

---

* Assistant Professor of Law, University of Nebraska College of Law. J.D., University of Chicago, 2007; M.A. (economics), George Mason University, 2010; B.A., St. John's College, 2003. With particular thanks to David Thaw, David Opderbeck, and participants of TPRC44 for tireless discussions and valuable feedback, and Will Nelson and Jared Koch for outstanding research assistance.

I. INTRODUCTION

We are in the midst of the latest iteration of the "Crypto Wars." These conflicts, nominally waged between the proponents of strong encryption technologies on the one hand and government interests on the other, are the natural result of increased availability and use of strong encryption throughout the communications ecosystem. Strong encryption makes it difficult, and in some cases effectively impossible, for the government to obtain information from individuals — even in cases where it has a lawful basis for demanding that information and a legitimate need to obtain access to it. The availability of a technology that effectively moots the government's ability to compel the disclosure of information shifts the established balance of power between individuals and the government. This Article uses the Communications Assistance for Law Enforcement Act ("CALEA"), a law adopted in 1994 during the previous iteration of the Crypto Wars, as a lens to understand how Congress can, and is likely to, respond to this changing balance of power.

The previous battle that occurred in the early 1990s came as digitalization of telecommunications and the proliferation of high-performance and low-cost computing platforms made the widespread use of encryption a possibility for the first time.[1] Law enforcement became increasingly unable to effectuate court-issued wiretap orders, leading to concern that technology would undermine basic law enforcement capabilities. At the same time, however, there was already an understanding that encryption technologies were going to be essential to the evolving market for "information services" — that is, for the then newly commercial Internet.[2] In 1994, Congress struck an important

1. *See infra* Section II.C.2.

2. *See* Peter H. Lewis, *Attention Shoppers: Internet Is Open*, N.Y. TIMES (Aug. 12, 1994), http://www.nytimes.com/1994/08/12/business/attention-shoppers-internet-is-open.html (last visited Apr. 10, 2017) ("Experts have long seen such iron-clad security as a necessary first step before commercial transactions can become common on the Internet . . . .").

compromise when enacting CALEA. CALEA requires telecommunications carriers to maintain certain capabilities historically available to assist law enforcement but otherwise allows them to design and deploy (and allow their customers to use) encryption as they see fit.[3]

But CALEA left many — really most — of the harder questions about encryption unanswered. At the time CALEA was adopted, the government believed that it had created a new standardized encryption system that addressed the immediate concerns about encryption, so any efforts to regulate encryption in CALEA were abandoned.[4] Its sole purpose was to maintain the government's extant capabilities to intercept wire communications at carrier facilities.[5] It made no attempt to address more complicated questions about how the nascent commercial Internet would affect the balance of power between individuals and the government, beyond saying that CALEA itself would not be the answer. Perhaps most importantly, CALEA was written in an era when the focus was still on intercepting communications traversing a centralized network of telecommunications switches.[6] Contemporary concerns about encryption have relatively little to do with intercepting information in transit, or even with accessing information stored by electronic communications services. Rather, they are increasingly focused on obtaining access to information stored on user-controlled devices or storage.

These questions have lingered in the background of Internet and technology policy debates for the past two decades, occasionally flaring into short-lived conflicts as Congress has considered communications-related legislation, or as law enforcement has expressed concerns about new technologies. But until recently there was relatively little appetite to rehash the earlier battles. This was largely because parties on both sides of the debate could live with the status quo established in the 1990s: The tech industry was free to deploy, and consumers were free to use, strong encryption. But since most users did not make substantial use of encryption at the time, the government could obtain access to significant amounts of their information — notably metadata[7] and stored data.[8]

This status quo has changed in recent years.[9] The Snowden revelations in particular upset the existing détente,[10] though the more substantial challenges to the status quo result from changing technology and

3. *See infra* Part III.
4. *See infra* Section V.B.1.
5. *See infra* Part III.
6. *See infra* Section IV.B.
7. Throughout this Article, I use "metadata" generally to refer to information about substantive communications. Different statutes refer to such information using different terms (for example, records, call-identifying information, etc.).
8. *See infra* Section VI.A.2.
9. *See infra* Section V.A.
10. *See infra* Section VI.A.2.

its uses.[11] Ironically, the most impactful of these revelations related to the government's bulk collection of *unencrypted* information, chiefly metadata. This, however, was enough to prompt substantial concerns about the lawfulness and legitimate extent of government data collection programs. In combination with revelations about National Security Agency ("NSA") efforts to weaken encryption and about the cooperation of technology firms like Apple with NSA programs, the revelation of government metadata collection also rekindled technologists' interest in deploying increasingly strong and pervasive encryption.[12] This, in turn, has renewed the government's concerns about maintaining its ability to obtain information from and about individuals.

With the détente over, these concerns rose to nationwide prominence in the recent fight between the Federal Bureau of Investigation ("FBI") and Apple over access to the contents of one of the San Bernardino shooters' encrypted iPhone.[13] Following the Snowden revelations, Apple began updating its various iPhone products to implement device-level end-to-end encryption. With this encryption, every aspect of an iPhone owner's use of that phone is encrypted. Critically, Apple has designed this encryption such that it has no ability to access the encrypted contents of a user's iPhone — the encryption is accomplished in part using a key that the user (and only the user) knows.[14]

One of the arguments forcefully advanced by Apple in its fight with the FBI was that CALEA dispositively addressed the issue, absolving Apple of any obligation to assist law enforcement in the decryption of a user's encrypted device.[15] As explained in Part III of this Article, this understanding is unequivocally wrong.[16] CALEA's text, statutory history, historical context, and subsequent judicial interpretation all make clear that it has little, if anything, to say about Apple's obligation to assist law enforcement in these cases. At the same time, CALEA is instructive in thinking about how Congress may approach the shifting

---

11. *See infra* Section V.A.

12. *Id.*; *see also NSA Prism Program Slides*, THE GUARDIAN (Nov. 1, 2013, 10:40 PM), https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document [https://perma.cc/XA2E-2XGQ] (highlighting Apple's cooperation with the NSA's PRISM program).

13. *See infra* Section V.A.4.

14. *See infra* Section VI.B.3.

15. *See* Apple Inc.'s Reply to Govt.'s Opposition to Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search at 7, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 5:16-cm-00010-SP (C.D. Cal. Mar. 15, 2016) ("The government seeks authority that Congress has expressly and impliedly rejected through CALEA."); *see also* Amicus Curiae Brief of Law Professors in Support of Apple, Inc. at 14, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 5:16-cm-00010-SP (C.D. Cal. Mar. 15, 2016) ("CALEA provides a detailed statutory scheme that specifies which kinds of companies must assist the government in its surveillance orders and what assistance those companies must provide.").

16. *See infra* Part III.

balance between individuals and law enforcement caused by the widespread use of encryption. Although this fight is currently unfolding in the courts, it is becoming increasingly clear that crafting a solution to these issues will require congressional input. Thus, it seems more and more likely that Congress will take up the problem of encryption in the coming years.

This Article uses CALEA as a lens to understand how Congress may approach the challenge of finding a new balance between the individual's right to be free from undue government intrusion and society's need to encroach occasionally upon that right. It considers a number of options, from the unlikely solution most often advanced by many in the government (for example, prohibiting the use of strong encryption or requiring "backdoor" access to encrypted information)[17] to the equally unlikely solution favored by many technologists (for example, fully liberalizing the use of strong encryption).[18] Debates over encryption have focused almost entirely on these two polar approaches to little avail; but as this Article explores, neither is satisfactory, and the binary nature of these options prevents serious consideration of more nuanced alternatives. This Article is an attempt to move beyond these entrenched positions, to find fertile ground for productive dialogue. In particular, this Article considers three possible, non-exclusive approaches to regulating encryption: requiring that (1) certain metadata be retained and made available to law enforcement in unencrypted form;[19] (2) mass-market platforms operating above a certain scale either not offer "strong" end-to-end encryption or retain the ability to disclose unencrypted content;[20] and (3) firms offering strong encryption make available certain pre-defined technical information about the implementation of the encryption system.[21] While requirements such as these are unlikely to make either those advocating for or those concerned about the availability of strong encryption happy, they are based on long-established legal norms and viable technological models. Perhaps most importantly, they preserve a balance between the rights of individuals and needs of the government.

This Article proceeds in five parts. Part II provides a brief technological and legal history of law enforcement efforts to obtain access to

17. *See infra* Section VI.A.1.

18. *See infra* Section VI.A.2.

19. *See infra* Section VI.B.1.

20. *See infra* Section VI.B.2. The term "strong" is used throughout this Article to describe the type of encryption at issue in policy debates. It is a term of art that refers to encryption that is sufficiently difficult to break using a "brute force" attack (that is, guessing keys) that it can be considered secure. *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY § 1.1 (Phil Sutherland ed., 2d ed. 1996) ("Cryptography is more concerned with cryptosystems that are computationally infeasible to break. An algorithm is considered computationally secure (sometimes called strong) if it cannot be broken with available resources, either current or future."). Encryption generally is discussed further in Section II.C.2.

21. *See infra* Section VI.B.3.

electronically stored and transferred information. Parts III and IV focus on CALEA, the most substantial legislative effort to date to address the effects of changing technologies — including the introduction of widely available encryption — on law enforcement access to such information. Part III addresses CALEA's purpose and structure. Part IV then reviews how CALEA has been applied as digital networks have continued to evolve. Part V builds on the discussion from Parts III and IV, using CALEA as a lens through which to understand the contemporary technical and political factors that have exacerbated the challenges that encryption poses to law enforcement. Part VI evaluates possible legislative approaches that Congress may take in regulating the use of strong encryption to maintain a balance between the allocation of the rights and burdens to individuals and to law enforcement.

II. A BRIEF TECHNOLOGICAL AND LEGAL HISTORY OF ACCESSING COMMUNICATIONS

A. The Telephone

The occasionally tense relationship between law enforcement and communications technology began with the advent of the telephone. Prior to the telephone, it was costly to communicate other than in person — whether in terms of time (letter writing was slow and the post even slower), money (telegraphs were priced by the word), or attention (both telegraphs and the post required interacting with others even for the most basic use cases). But by the early 1900s, the rapid growth in the telephone market was quickly bringing near-instantaneous, relatively low cost, and convenient communications to everyone.[22]

This new technology changed the law's relationship with communications as well. Prior to the telephone, law enforcement tended to focus on message senders and recipients, not communications intermediaries. If a message was given to a common carrier like the post, it was largely protected from government interception.[23] But the focus on the sender or receiver instead of the carrier was as much a practical result as a legal one: It was simply easier to obtain information from the sender or recipient of a letter than from the letter carrier.

---

22. *See* Richard Gable, *The Early Competitive Era in Telephone Communication, 1893–1920*, 34 LAW & CONTEMP. PROBS. 340, 344–46 (discussing growth of service and decline of prices in the telephone market circa 1900, and noting that "[o]ut of 1,051 U.S. cities with a 1902 population greater than 4,000, 1,002 had telephone facilities").

23. *See Ex parte* Jackson, 96 U.S. 727, 733 (1877) (1969) ("Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.").

The telephone changed this balance. With the telephone, it was much easier to obtain information by tapping directly into the communications network.[24] This could be done surreptitiously and at relatively low cost.[25] It also was arguably necessary to take this approach to scale the government's surveillance capabilities with the growth of communications made possible by the telephone.[26] Critically, unlike earlier forms of telecommunications, the telephone left no physical record that could be obtained at a later time by a search of the sender or recipient of a communication; in order to obtain telephone communications, the government had to obtain them at the moment of transmission.

The Supreme Court addressed this changing technological balance in several cases during the twentieth century. Key among these cases are *Olmstead*,[27] *Katz*,[28] and *Smith*.[29] In *Olmstead*, the Court first faced the question of whether telephone wiretaps were subject to Fourth Amendment protection. The Court found that they were, explaining that the Fourth Amendment is not violated "unless there has been an official search and seizure of [an individual's] person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."[30] But in the case of the telephone, the Court found, "[t]here was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[31] The Court therefore held that wiretapping "did not amount to a search or seizure within the meaning of the Fourth Amendment."[32]

Olmstead was the law of the land for four decades, but its reasoning was flatly rejected in *Katz*. By the time of *Katz*, "[t]he premise that property interests control the right of the Government to search and seize ha[d] been discredited."[33] The Court observed:

> Although a closely divided Court supposed in Olmstead that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested.

---

24. *See* WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 174–75 (2d ed. 2007).

25. *See id.* (describing the electronic surveillance as "invisible to the target" and leaving no "telltale 'marks on the envelope'").

26. *See id.* (describing the ubiquity of electronic communications).

27. Olmstead v. United States, 277 U.S. 438 (1928).

28. Katz v. United States, 389 U.S. 347 (1967).

29. Smith v. Maryland, 442 U.S. 735 (1979).

30. *Olmstead*, 277 U.S. at 466.

31. *Id.* at 464.

32. *Id.* at 466.

33. *Katz*, 389 U.S. at 353 (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967)).

> Indeed, we have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, over-heard without any "technical trespass under . . . local property law."[34]

The Court went on to draw a new line, establishing what are now central tenets of Fourth Amendment jurisprudence: that the Fourth Amendment protects people, not property,[35] and that it applies in instances where individuals have a reasonable expectation of privacy.[36]

Even more important for the purposes of the present debates, however, is the scope of the *Katz* court's opinion. *Katz* addressed the application of the Fourth Amendment to the interception of conversations — the substantive content of a communication. *Katz* did not address what we would think of today as metadata — information about a conversation.

A decade after *Katz*, the Court addressed the question of metadata in *New York Telephone Co*.[37] Here, the Court stressed the difference between wiretaps and pen registers.[38] Wiretaps, the subject of *Katz*, are used to obtain the contents of a communication. Pen registers, however, are devices that record non-content information about a telephone call, such as the numbers dialed to establish the call.[39]

This distinction between intercepting the contents of a call and recording information about the numbers dialed was critical two years later in *Smith*, in which the Court held that information obtained through the use of a pen register is not protected by the Fourth Amendment.[40] The Court, citing *New York Telephone Co.*, explained that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."[41] The Court went on to find that phone numbers, and other non-content information, are routinely turned over to third parties in the ordinary course of business, and that there is no objectively reasonable

---

34. *Id.* (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

35. *Id.* at 351.

36. *Id.* at 360–61 (Harlan, J., concurring).

37. United States v. N.Y. Tel. Co., 434 U.S. 159 (1977).

38. *Id.* at 167.

39. *Id.* ("Pen registers . . . do not acquire the 'contents' of communications . . . ."); *see also id.* at 161 n.1 ("A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.").

40. Smith v. Maryland, 442 U.S. 735 (1979). This follows the logic of *Ex Parte Jackson*, which held that the contents of letters in the mail are guarded from examination, but that the "outward form and weight" of the letters are not. 96 U.S. 727, 733 (1877).

41. *Smith,* 442 U.S. at 741.

expectation of privacy in such information.[42] Applying *Katz*, the Court held that Fourth Amendment protections do not extend to what we would today call metadata — functional information used in the operation of products or services.[43]

B. The Early Statutes

Through *New York Telephone Co.* and *Smith*, the Court recognized a constitutionally meaningful distinction between content and metadata. In doing so, it was following a path charted by Congress.

In response to *Katz*, Congress adopted the first Wiretap Act as Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[44] The Act prohibited "the interception of a wire or oral communication" by law enforcement without a court order and specified requirements for obtaining such an order that were substantially more stringent than the constitutional requirements imposed by the Fourth Amendment.[45] It was this Act that the Court was interpreting in *New York Telephone Co.* when it recognized the distinction between what wiretaps obtain (content) and what pen registers obtain (metadata) — a holding that was reinforced in *Smith* when the Court recognized that information obtained by pen registers is not protected by the Fourth Amendment.

Congress has continued to maintain this distinction. With the Electronic Communications Privacy Act of 1986 ("ECPA"), Congress substantially revised the Wiretap Act and added the Stored Communications Act and Pen Register Act.[46] The revised Wiretap Act continued to focus on the content of communications while the new Pen Register Act specifically addressed the use of pen registers and similar devices to obtain information about calls.[47] The Stored Communications Act addressed access to both the content of and metadata relating to electronic information stored by electronic communications services, but it applied substantially different standards to each.[48] Similarly, in

---

42. *Id.* at 743–44. This is known as the third-party doctrine. *See generally* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

43. *Smith,* 442 U.S. at 743–44.

44. *See* Pub. L. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2520 (2012)).

45. *Id.* § 802 (codified as amended at 18 U.S.C. §§ 2511, 2518 (2012)). Note that the Act also prohibited intercept by private parties.

46. Pub. L. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2520, 2701–2712, 3121–3127 (2012)).

47. *Compare* 18 U.S.C. § 3127(3) ("'[P]en register' means a device or process which records or decodes dialing, routing, addressing, or signaling information . . . provided, however, that such information shall not include the contents of any communication . . . ."), *with* 18 U.S.C. § 2510(4) ("'[I]ntercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication . . . .").

48. *Compare* 18 U.S.C. § 2703(a) (relating to disclosure of the *contents* of communications), *with* 18 U.S.C. § 2703(c) (relating to disclosure of *records about* communications).

CALEA Congress imposed different requirements upon telecommunications carriers relating to the ability to "intercept . . . communications"[49] in contrast to merely "enabling the government . . . to access call-identifying information . . . ."[50] Congress has continued to recognize this distinction in subsequent statutes.[51]

Importantly, none of these statutes impose any obligations relating to encryption.[52] Rather, they address only the circumstances under which third parties need to provide the government with access to information or to facilities needed to obtain information, be that information substantive content or metadata. There is a straightforward reason that these statutes do not address encryption: at the time of their drafting, encryption was not a widely available technology, and it was not provided as a service by communications providers to their customers. To the extent that the idiosyncratic subject of a warrant was using encryption in her communications, third-party communications and storage providers would not be in any particular position to assist in decrypting those communications; indeed, given the state of the technology at the time, they would not be in any position to systematically prevent — let alone detect — the use of encryption.[53] In these one-off situations it would therefore fall to the government and the subject of its warrant to address any encryption concerns.

Under these provisions of the Stored Communications Act, compelling disclosure of the content of communications generally (but not always) requires a warrant issued pursuant to the Federal Rules of Criminal Procedure, whereas disclosure of records about communications can be compelled subject only to administrative process and, in the case of certain records, subject to even less process.

49. 47 U.S.C. § 1002(a)(1) (2012).

50. *Id.* § 1002(a)(2).

51. *See, e.g.*, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). It may be objected that Congress has only adhered to these distinctions in light of the different treatment under Fourth Amendment jurisprudence for accessing these types of information (that is, the differing levels of access protection for data and metadata). But this objection is not convincing, given that Congress has elected not to extend statutory authorization of wiretaps to the fullest extent allowed by the Fourth Amendment. *See* 18 U.S.C. § 2518 (2012) (imposing requirements for obtaining a wiretap).

52. CALEA's treatment of encryption is discussed extensively below. *See infra* Section V.B.1.

53. Detecting such communications requires telecommunications switches that are capable of "deep packet inspection" — that is, computationally evaluating the content of digital communications in real time. Switches capable of doing this in a sophisticated way were not developed until the early 2000s. *See, e.g.*, Fang Yu et al., *Fast and Memory-efficient Regular Expression Matching for Deep Packet Inspection*, Proc's ACM/IEEE Symp. on Architecture for Networking and Commc'ns Systems (2006) (discussing research necessary to the development of the sort of deep-packet inspection technologies needed to detect encryption in real time). Moreover, it is particularly difficult to identify *encrypted* communications, as a goal of encryption is to transform information into a form that is indistinguishable from random information. *See infra* note 60.

C. Subsequent Concerns

Computer and communications technology has continued to advance at a rapid pace since Congress's adoption of these early statutes. Indeed, changes with which we are struggling today were already afoot contemporaneously with the adoption of the ECPA and were recognized, if not necessarily addressed, by CALEA. Key among these changes were the digitalization of communications and the increased availability and usability of encryption technologies.

1. Digitalization

One of the major projects of the 1980s was digitalization of the telephone network. The effort began during the monopoly era of the Bell System with the development of the transistor in 1948 and the T-Carrier transmission line in 1962.[54] These transmission lines transmitted voice calls as digital signals, and marked the beginning of transitioning the telephone network to digital transmission and switching technologies.[55] By the late 1980s, most inter-office and long-distance circuits were digital; only the last-mile connections, between customer premises and the customer-facing telephone switch, were still analog.[56] By 1988, a consumer-facing digital technology, Integrated Services Digital Network ("ISDN"), had been developed in expectation of an eventual transition of all telephone circuits to digital technology.[57]

The transition to a digital network enabled a number of new features, such as call forwarding, and created technical challenges to effectuating authorized surveillance.[58] As explained in the House Report on CALEA:

> Indeed, until recently, the question of system design was never an issue for authorized surveillance, since intrinsic elements of wire lined networks presented access points where law enforcement, with minimum assistance from telephone companies, could isolate the communications associated with a particular surveillance target and effectuate an intercept. Where problems did arise, they could be addressed on a case-

54. F.M. SMITS, A HISTORY OF ENGINEERING & SCIENCE IN THE BELL SYSTEM: TRANSMISSION TECHNOLOGY (1925–1975), at 527, 562–63 (1975).

55. *Id.*

56. *Id.*; *see also* Gordon Bell & Jim Gemmell, *On-ramp Prospects for the Information Superhighway Dream*, 39 COMM. ACM 55, 56 (1996) ("The *last-mile* problem is the major barrier to the Information Highway.").

57. ANTON A. HUURDEMAN, THE WORLDWIDE HISTORY OF TELECOMMUNICATIONS 505 (2003).

58. *See infra* Section III.A.

> by-case basis in negotiations between the local monopoly service provider and law enforcement . . . . The break-up of the Bell system and the rapid proliferation of new telecommunications technologies and services have vastly complicated law enforcement's task in that regard.[59]

A worry that the advent of digital transmission and switching technologies was frustrating longstanding law enforcement capabilities was among the core concerns that led Congress to adopt CALEA in 1994. Digitalization generally, as well as the effects that it had on law enforcement in particular, is discussed further in Section III.A.

2. Encryption

Research into strong encryption technologies expanded following World War II.[60] By the 1970s, key parts of modern symmetric- and

---

59. H.R. REP. NO. 103-827, at 15–16 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3494.

60. One of the first rules of computer security is that one should use existing, well-tested implementations of complicated code wherever possible, as opposed to re-implementing a new version of that code in new applications. In that spirit, this Article does not offer a comprehensive background explanation of what encryption is. *See generally* Weisiyu Jiang, *Public Key Encryption*, 1 GEO. L. TECH. REV. 105 (2016); Gus Hurwitz, *Understanding Encryption: No Longer Just About Sending Secret Messages*, TECHPOLICYDAILY.COM (Oct. 21, 2015), http://www.techpolicydaily.com/technology/encryption-secret-messages/ [https://perma.cc/DKJ4-H7KA]. For in-depth background, see generally AN INTRODUCTION TO CRYPTOGRAPHY (1999) (ebook), *available at* https://courses.cs.vt.edu/cs5204/fall09-kafura/Papers/Security/IntroToCryptography.pdf [https://perma.cc/R4N5-SET4]. The canonical texts are SCHNEIER, *supra* note 20, and NIELS FERGUSON, BRUCE SCHNEIER & TADAYOSHI KOHNO, CRYPTOGRAPHY ENGINEERING (Carol Long, Tom Dinse & Daniel Scribner eds., 2010).

In very general terms, encryption is a mathematical process whereby intelligible information is transformed into near-unintelligible form. Ideally, encrypted information is indistinguishable from random noise. The equations used in this transformation rely on variables called "keys" — keys are nothing more than (typically very long) numbers. The defining characteristic of these equations is that it does not take very long to encode or decode information if you know the keys, but it takes a very long time to decode encrypted information if you do not have the key — and this gap between how long it takes to decode information with and without the key can be arbitrarily increased by using longer and longer keys. The reason that it takes so long to decode encrypted information without the key is that strong encryption can be broken only by guessing keys. The process of trying random keys to decode encrypted information is known as a "brute force" attack. To put this challenge in perspective, a modern encryption algorithm may take a modern computer one second to encrypt a piece of information; decoding that information without the key could easily take that same computer a million times longer than the universe has existed. For this reason, most successful attacks on encryption take advantage of mistakes in the code that programmers write to implement encryption equations. *See generally* Ross Anderson, *Why Cryptosystems Fail*, 37 COMM. ACM 32 (1994).

Depending upon the specific type of encryption, there are different types of keys. Perhaps most important, some encryption algorithms use "symmetric" keys, where the same key that

asymmetric-key encryption technologies had been developed. The Data Encryption Standard ("DES") — a symmetric-key encryption algorithm developed by IBM — was adopted as the first standardized encryption algorithm by the United States government in 1977.[61] While no longer considered a strong algorithm, DES set the stage for the widespread use of encryption to store data securely.[62] Contemporaneously, researchers in the United States and UK were developing the first public-key encryption algorithms — Diffie-Hellman and RSA — which are today essential for securely transmitting information over the Internet.[63]

The potential for encryption to interfere with legitimate government needs was clear even in the early days of modern encryption,[64] but that potential would remain largely hypothetical for several decades. Encryption was primarily used by large corporations and firms dealing with sensitive information, such as banks, energy firms, and hospitals.[65] Even though encryption algorithms were available, the lack

---

encrypts information also decrypts it; other algorithms use "asymmetric" keys, where one key is used to encrypt information but another key is needed in order to decrypt it.

Both symmetric- and asymmetric- key encryption can be used to keep information confidential. Asymmetric-key encryption has the added benefit that it can be used for authentication. If the encryption key is made public, then anyone can encode messages that only the party holding the (still secret) decryption key can read. This is useful, for instance, when logging in to a bank's webpage: the user encrypts their username and password with the bank's public key, knowing that only the bank will be able to decode the username and password. Alternatively, the decryption key can be made public and the encryption key kept secret. This allows the person decrypting the information to know who sent it. This is called "signing" the information, and is used, for instance, by Microsoft sending updates to users' computers; if the user can decrypt the information using Microsoft's public key, they know that the update is authentic and was sent by Microsoft.

61. *See generally* DIFFIE & LANDAU, *supra* note 24, at 66–68; SCHNEIER, *supra* note 20, at 265–301; A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 735–36 (1995) (discussing adoption of DES as the federal standard for encryption).

62. Froomkin, *supra* note 61, at 738; *see also* ROSS ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 158 (Carol Long, Tom Dinse & Tim Tate eds., 2d ed. 2008); FERGUSON ET AL., *supra* note 60.

63. *See generally* Greg Vetter, *Patenting Cryptographic Technology*, 84 CHI.-KENT L. REV. 757, 761–63 (2010); *see also* DIFFIE & LANDAU, *supra* note 24, at 68–69; FERGUSON ET AL., *supra* note 60, at 181, 195.

64. This was particularly true in the national security context, where there were concerns that use of encryption by other countries would both assist them and limit our own signal intelligence capabilities. For this reason, encryption was classified as a munition subject to substantial export restrictions. DIFFIE & LANDAU, *supra* note 24, at 120–23; Bernadette Barnard, *Leveraging Worldwide Encryption Standards via U.S. Export Controls: The U.S. Government's Authority to "Safeguard" the Global Information Infrastructure*, 1997 COLUM. BUS. L. REV. 429, 439–443 (1997) (discussing regulation of encryption under the Arms Export Control Act and Export Administration Act); *see also* SCHNEIER, *supra* note 20, at 278–85 (discussing concerns that the NSA had interfered in the design of DES, incorporating design flaws into the algorithm that the government would be able to exploit to decrypt information).

65. DIFFIE & LANDAU, *supra* note 24, at 47–48.

of a robust digital network infrastructure typically made it easier to protect all but the most sensitive data by securing physical access to systems, and the computational complexity of encryption made its use relatively unattractive given the limited power of contemporary computers. Indeed, even as export restrictions — the primary form of regulation to which encryption has been subject — fell away in recent years, the slow adoption of encryption has surprised many.[66]

By the early 1990s, however, it was clear that widespread use of encryption, and all of the challenges that it posed for government, was looming over the horizon. Telecommunications networks were increasingly digital. The cost of computers was falling and their power increasing; they were becoming a common home appliance. The commercialization of the Internet pointed to a future filled with online commerce that would need to be protected by encryption.[67] Perhaps the most telling harbinger was AT&T's development of the TSD-3600, a commercially available secure telephone that encrypted phone calls in real time, using encryption that would be very difficult even for the NSA to break.[68]

This led to a series of fights into the early 1990s between encryption researchers and civil libertarians, on the one hand, and the government on the other. Among these fights were challenges to the government's export restrictions on encryption software[69] and the government's effort to develop the Escrowed Encryption Standard, an encryption system that would allow the government to decrypt encrypted communications.[70] The government lost both of these fights. Efforts to restrict the distribution of encryption-related research ran into trouble on First Amendment grounds.[71] Compounding these difficulties facing regulators, in 1996 President Clinton signed Executive Order 13026, which transferred encryption export controls from the State Department

66. *Id*. at 257 ("Contrary to the expectation of many of its fans, the deregulation of cryptography [in January 2000] did not produce any immediate explosion in either the number of available cryptographic products or the frequency of their use. Anyone who expected most email and phone calls to be encrypted overnight was surely disappointed.").

67. Prior to the early 1990s, the Internet — really, an internet run by the NSF — was used solely for government and university research, with any commercial activity strictly prohibited. Starting in 1992, the NSF began the process of transferring management of this internet to a consortium of private parties, expressly anticipating that commercial uses would be allowed under the new arrangement. This process, to which we owe the modern commercial Internet, was completed in 1995. *See generally,* Brett Frischmann*, Privatization and Commercialization of the Internet Infrastructure*, 2 COLUM. SCI. & TECH. L. REV. 1 (2001).

68. *See infra* Section V.B.1.

69. *See* Bernstein v. United States Dep't of Justice, 176 F.3d 1132, 1136 (9th Cir. 1999); *see also* David McClure, *First Amendment Freedoms and the Encryption Export Battle: Deciphering the Importance of* Bernstein v. United States Department of Justice*, 176 F.3d 1132 (9th Cir. 1999)*, 79 NEB. L. REV. 465 (2000).

70. *See infra* Section V.B.1.

71. *See Bernstein*, 176 F.3d. at 1144 (holding that government export restrictions on the distribution of encryption source code constituted an impermissible prior restraint of constitutionally-protected speech).

as a "munition" to the Commerce Department as a "commercial technology," substantially reducing export controls on encryption.[72] Critical flaws were also found in the Escrowed Encryption Standard, rendering it unsuitable for use and leading the way to commercial adoption of stronger encryption.[73]

These fights were reflected in the drafting of CALEA. As initially drafted, CALEA would have imposed substantial limits on the use of encryption by telecommunications carriers. But in light of the development of the Escrowed Encryption Standard, Congress and the FBI believed that any immediate concerns about encryption had been addressed.[74] In order to avoid a legislative fight, any regulation of encryption was removed and CALEA was left to focus solely on ensuring that law enforcement had access to communications transiting telecommunications networks, even if that only meant access to encrypted communications.[75] The eventual position adopted by CALEA is expressly permissive towards the use of encryption, both in the statutory language[76] and the legislative history.[77] At the same time, it is a gross misstatement to say that CALEA deregulated the use of encryption. CALEA did nothing to affect then existent technologies, and it certainly did not give carte blanche to future technologies.[78]

3. Today's Debate

The general outcome of the Crypto Wars of the 1990s was a resounding victory for proponents of strong encryption; the content of communications could be protected by strong encryption, and companies and individuals were broadly free to design and implement encryption technologies. But the context of today's debates about encryption is substantially different than it was nearly twenty-five years ago. At the time CALEA was being debated, state of the art personal computers ran Windows 3.1 on 16 megabytes of RAM and connected to the Internet at a maximum speed of 14.4 kilobits per second via services such

72. Exec. Order No. 13026, 61 Fed. Reg. 58,767 (Nov. 19, 1996).

73. *See, e.g.*, Matt Blaze, *Protocol Failure in the Escrowed Encryption Standard*, 2ND ACM CONFERENCE ON COMPUTER & COMMC'N SECURITY (1994); *see also* Section V.B.1.

74. *See infra* note 231 and accompanying text (discussing how Congress and the FBI forewent requiring decryption assistance obligations in CALEA on the belief — which was ultimately proved incorrect — that adoption of EES would address this concern).

75. *See infra* Section V.B.

76. 47 U.S.C. § 1002(b)(3) (2012).

77. *See* H.R. REP. NO. 103-827, at 1 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3489 ("A telecommunications carrier shall not be responsible for decrypting . . . any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."); *see also id.* at 24, *reprinted in* 1994 U.S.C.C.A.N. 3489, 3504 ("Finally, telecommunications carriers have no responsibility to decrypt encrypted communications . . . unless the carrier provided the encryption and can decrypt it.").

78. *See infra* Section VI.B.2.

as CompuServe and Prodigy.[79] Phone lines did not connect users directly to the Internet; they connected them to separate Internet Service Providers, which in turn connected users to the Internet. [80] With these capabilities it would take a week to transmit a 1 gigabyte movie.[81] But one would never do that because most hard drives were only half a gigabyte, and most consumer computers weren't powerful enough to play video (indeed, most personal computers couldn't even play music).[82] When the few people with online accounts weren't using them, they would disconnect their computers from the network. Further, when people weren't using their computers, they would turn them off.

It is no surprise that present debates over encryption are different than they have been in the past. Today we live in the era of smartphones and wireless connectivity. Almost all Americans carry powerful computers (their phones) with them everywhere they go. These computers are almost always turned on and connected to the Internet. They are used for communications, information collection and storage, Internet access, social activity, and even finances.

In contrast with the state of the technology twenty-five (or even ten) years ago, almost every aspect of modern computing can be — and often is — seamlessly integrated into a single device and a single user experience. At the time CALEA was adopted, for the typical user, connecting to the Internet would involve turning on a computer, using a modem to connect to a service like CompuServe, running a specific application to connect to the Internet (as opposed to CompuServe's own proprietary network), and then accessing one of a relatively small number of online resources. Each of these was a discrete step; nothing about it was seamless, either from a technological or a user experience perspective.

This difference is central to understanding how debates about encryption have changed. Encryption used to be difficult to use, and each step of an interaction would require separate encryption efforts. A remarkably sophisticated user may have been able to string together a series of interconnected applications to create what we today call "end-to-end" encryption. But it would have been extremely clumsy. Perhaps even more importantly, it would have been relatively useless, given how few other people and services were online at the time. The online world represented a very small portion of the lives of even those power

---

79. *See, e.g.*, *Comparing Today's Computers to 1995's*, RELATIVELY INTERESTING (Feb. 23, 2012), http://www.relativelyinteresting.com/comparing-todays-computers-to-1995s/ [https://perma.cc/SN3B-739Y].

80. *See, e.g.*, *In re* Commc'ns Assistance for Law Enf't Act & Broadband Access & Servs., 19 F.C.C.R. 15676, 15677–78 (2004) (describing Internet access at the time CALEA was enacted).

81. Under ideal conditions, a 14.4 kilobits per second modem can transmit 6.48 megabytes per hour, which is equal to 155.5 megabytes per day or 1.08 gigabytes per week.

82. *See Comparing Today's Computers to 1995's*, *supra* note 79.

users whose Internet usage was disproportionately high relative to the median user. Today, by comparison, Internet-connected devices are ubiquitous. Applications and services increasingly offer seamless, integrated experiences across devices, and these devices are increasingly integrated into our day-to-day lives. Today, the online world represents a very substantial portion of the lives of even those who spend most of their time offline.

The role of encryption in the current technological reality is fundamentally different than it has been in the past. These are new issues, not previously considered by Congress. The various sorts of service providers covered by ECPA and CALEA had not previously offered end-to-end encryption capabilities; at most, they would provide storage for information encrypted by a third party. And while CALEA contemplated encryption of communications, telecommunications carriers have generally not managed the storage of those communications by parties on either end of the channel. Perhaps most importantly, the prospect of firms offering turnkey, integrated encrypted communications and storage capabilities is entirely new. It represents a far more dramatic shift in the relationship between the rights of individuals and the needs of law enforcement than any previous change in communications technology.

The remainder of this Article uses Congress's past efforts — most notably CALEA — to consider how it may approach these new issues.

III. CALEA'S PURPOSE AND STRUCTURE

Compelled disclosure of, or access to, information presents difficult political and legal questions. As Congress and the courts have answered these questions over the years, the technological solutions have been found to implement these legal requirements. Prior to widespread digitalization of data and communications, such implementation was relatively straightforward because there were clear functional delineations separating data held by users, data held by remote information services, and data transmitted by telecommunications. Telephone switches, for instance, were passive carriers of analog audio signals between endpoints. As a technical matter, it is relatively easy to record information traversing analog switches in real time.[83] To access stored information one looks to the entity that holds that information and demands access either subject to a warrant or subpoena (in the event the information is under the control of the subject of an investigation), or the Stored Communications Act (in the event that information is under

83. *See*, *e.g.*, Paul Rosenzweig, *The Evolution of Wiretapping*, 12 ENGAGE: J. FEDERALIST SOC'Y PRAC. GROUPS 83 (2011); Whitfield Diffie & Susan Landau, *Communications Surveillance: Privacy and Security at Risk*, 52 COMM'N ACM 42 (2009).

the control of a third party).[84] To get access to communications in transit, one looks to the telecommunications provider under the Pen Register or Wiretap Acts.

Digitalization of data made this relationship more complicated. In digital networks, telecommunications providers alter the format of analog audio signals, encoding them into digital information.[85] Once in this format, telecommunications switches actively process and retransmit the information traversing the network — they can even give users control over how that information traverses the network, for instance using features like call forwarding or redirection. What's more, the information from a single call may be multiplexed with other information traversing the network, making it difficult to isolate, let alone intercept, a single target call — unless the switches have been designed with such capabilities in mind. And, once calls are in digital form, it becomes much easier for the telecommunications network to manipulate information traversing it. This opens the door to telecommunications providers offering information services alongside — or built into — their networks, further blurring the previously clear lines. Suddenly, obtaining a copy of a conversation — such as pursuant to a wiretap order — requires tracing a call to a specific switch as it is directed (and redirected) through the network and then decoding and isolating a specific call from other information traversing that switch. This, in turn, may require that switches be designed with specific capabilities that would not otherwise have been incorporated into the switch design.

CALEA was Congress's first attempt to address how these technological changes affected the burdens placed upon the various parties in the communications ecosystem. As such, even though CALEA is not itself directly relevant to today's debates about encryption (as explained below), it is a useful starting point in understanding how Congress may respond to today's issues. This Part looks to CALEA's purpose and structure. It begins by explaining the problem that CALEA was written to address. It then looks at what CALEA does: the requirements CALEA imposes on telecommunications carriers. It concludes by looking at what CALEA does *not* do, a useful inquiry given the range of meanings often attributed to CALEA.

---

84. In federal civil litigation, for instance, disclosure of such information from a litigation party is governed by Rules 26 and 34. *See* Fed. R. Civ. Proc 26 & 34. In federal criminal investigation and litigation, it is governed by Rules 16, 17 and 41, and the 4th Amendment. *See* Fed. R. Crim. Proc. 16, 17, 41; U.S. CONST. amend. IV. The Stored Communications Act, 18 U.S.C. §§ 2701–11, governs disclosure of electronic communications held by third party electronic communications services. *See, e.g.*, 18 U.S.C. § 2702(a) (2012).

85. For an overview of the mechanics of digital networks, see SMITS, *supra* note 54.

A. The Problem CALEA Addresses

CALEA is an exceptionally technical statute, specifying detailed capabilities that the communications switches used by specific telecommunications carriers need to support. Yet CALEA was written to address a relatively straightforward problem: As the telephone network transitioned from analog to digital communications, it was increasingly difficult for telecommunications carriers to implement court-ordered wiretaps.[86] CALEA was meant to address this problem by requiring that telecommunications carriers use equipment capable of supporting wiretapping capabilities.[87]

Before looking in more detail at what CALEA does, it will be useful to discuss why it was necessary.

The traditional telephone network is a "circuit-switched" network. This means that when one person calls another they are given a dedicated communications channel. For much of the history of the network, this channel was, literally, a circuit: a loop of wire from one person's telephone that ran to a telephone switch which connected via another loop of wire to another's telephone.[88] In effect, each party's phone was directly connected to the other party's phone. Longer distance connections were facilitated using amplifiers that amplified the electrical charge traversing long circuits, but the underlying principle was the same: each call was allocated a dedicated electrical circuit that directly connected the parties' phones.[89]

This connection was the quintessential "dumb pipe" — other than occasionally amplifying the signal, the telephone carrier did not (and, indeed, could not) alter the signal in any way. This also made it exceptionally easy to wiretap calls; as a technical matter, one needed only

---

86. *See* Am. Council on Educ. v. Fed. Commc'ns Comm'n, 451 F.3d 226, 227–28 (D.C. Cir. 2006) ("Before the dawn of the digital era, there were few technological obstacles to the government's wiretapping capabilities. . . . Responding to . . . changing technologies, . . . Congress passed CALEA, which requires 'telecommunications carriers' to 'ensure' that their networks are technologically 'capable' of being accessed by authorized law enforcement officials.") (citing 47 U.S.C. § 1002(a)); H.R. REP. NO. 103-827, at 1 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3489 (declaring the act's purpose as "preserv[ing] the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding . . . , while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services").

87. *See* H.R. REP. NO. 103-827, at 1, *reprinted in* 1994 U.S.C.C.A.N. 3489, 3489; *see also* 47 U.S.C. § 1002(a)(1) (2012).

88. *See* PETER W. HUBER, MICHAEL K. KELLOGG & JOHN THORNE, FEDERAL TELECOMMUNICATIONS LAW § 14.2.12.6.1 (2d ed. 2016); STEVEN BELLOVIN ET AL., SECURITY IMPLICATIONS OF APPLYING THE COMMUNICATIONS ASSISTANCE TO LAW ENFORCEMENT ACT TO VOICE OVER IP 5 (2006), https://www.cs.columbia.edu/~smb/papers/CALEAVOIPreport.pdf [https://perma.cc/U74G-4R7G].

89. *See* SMITS, *supra* note 54.

touch a wire running to a speaker or recording device to the wires comprising the electrical circuit between the phones.[90] Those on the call might notice a slight decrease in volume, but there would be no effect beyond that.

This all began to change with the advent of digital communications in the 1960s and 1970s. There is no dedicated electrical circuit in digital communications. Rather, the analog voice signal is encoded into a digital signal at the transmitter end. That signal is then passed through the telephone network through a series of digital switches that are programmed with special routing protocols until it reaches its destination. At that point it is turned back into an analog signal for the receiver.[91]

The core challenges that digitalization presented for law enforcement starting in the 1980s were not actually related to the encoding of the communications channel. Indeed, until relatively recently, most phone calls were still analog between a customer's telephone and their carrier's central office; it wasn't until the call hit the first switch that it was encoded in digital form.[92] Rather, concerns related to how calls were routed through the telephone network.[93] In the 1980s, as telecommunications carriers began pushing digital switch technology to the edge of their networks, consumers gained increasing access to advanced routing features. For instance, they could set up call forwarding, which would allow a telephone user to dial one number but be connected to another number, or speed dialing, which would allow a user to "dial" a complete phone number by entering only a short code on his or her dial pad.[94] The caller could also use related features that would allow her to redirect a call to one number after dialing an initial number.

---

90. *See* BELLOVIN ET AL., *supra* note 88; HUBER, *supra* note 88, at § 14.2.12.6.1; MICAH SHERR ET AL., CAN THEY HEAR ME NOW? A SECURITY ANALYSIS OF LAW ENFORCEMENT WIRETAPS (2009), http://www.crypto.com/papers/calea-ccs2009.pdf [https://perma.cc/8NUM-YDNR]; Susan Landau, *The Large Immortal Machine and the Ticking Time Bomb*, 11 J. TELECOMM. & HIGH TECH. L. 1, 16 (2013).

91. *See generally* SMITS, *supra* note 54.

92. *See* HUBER, *supra* note 88, at § 14.2.12.6.2.

93. *See* OFFICE OF TECH. ASSESSMENT, ELECTRONIC SURVEILLANCE IN A DIGITAL AGE 2–4 (1995), https://www.princeton.edu/~ota/disk1/1995/9513/9513.PDF [https://perma.cc/T568-4F6N] ("Even the concept of the 'telephone number,' which [once] identified the target subject of the court-ordered wiretap and . . . a physical location, may now only be a number that begins the communication, then loses its identity with an individual or location as the call may be routed to others . . . .").

94. *See* H.R. REP. NO. 103-827, at 1 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3489 (noting that the purpose of CALEA is to preserve the ability to conduct intercepts in light of, among other things, "features and services such as call forwarding, speed dialing and conference calling"); COMM. TO STUDY NAT'L CRYPTOLOGY POLICY, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 218 (Kenneth W. Dam & Herbert S. Lin eds., 1996) ("New telecommunications services (e.g., call forwarding, paging, cellular calls) and others expected in the future have diminished the ability of law enforcement agencies to carry out legally authorized electronic surveillance."); FED. BUREAU OF INVESTIGATION, BENEFITS AND COSTS OF LEGISLATION TO ENSURE THE GOVERNMENT'S CONTINUED CAPABILITY TO INVESTIGATE CRIME WITH THE IMPLEMENTATION OF NEW TELECOMMUNICATIONS

These and similar features are problematic for law enforcement. A traditional wiretap can receive only the information sent on the wires between the subject's phone and the switch. Before the advent of digital transmission and switching, this provided law enforcement with all of the information about a given call. But modern switches use separate signaling channels to implement features like call forwarding and call redirection.[95] As a result, a wiretap does not capture all of the signaling information being sent to the network, or the resulting changes this information has on the call's routing through the network.[96] Law enforcement needs to know as much of this information as possible in order to ensure that they are intercepting all relevant communications and to screen out irrelevant communications.[97] For instance, with speed dialing or call forwarding, law enforcement would not be able to tell from dialed numbers alone who was being called, which could require them to deem a call irrelevant and discontinue monitoring it.[98] With the ability to redirect calls, the subject of a wiretap could initially dial an "irrelevant" number (again requiring discontinuation of monitoring by law enforcement) and then redirect the call to an otherwise-monitored target.

Both the FBI and the Government Accountability Office ("GAO") presented studies to Congress to measure the extent of this problem. FBI Director Louis Freeh reported that the FBI had identified 183 recent instances in which digital switching had interfered with a federal, state, or local law enforcement agency's ability to carry out a lawful wiretap order.[99] The GAO study concluded "that there are legitimate

---

TECHNOLOGIES (1992), *as reprinted in* BRUCE SCHNEIER & DAVID BANISAR, THE ELECTRONIC PRIVACY PAPERS 192 (1997) (discussing how features such as call forwarding, speed dialing, and automatic re-dial "frustrate or diminish the full interception as authorized").

95. This is called "out of band" signaling. Prior to the 1980s, telecommunications carriers used "in band" signaling, where codes that controlled the behavior of telecommunications switches were transmitted on the same line that callers used to speak to each other. *See* HUBER, *supra* note 88, at § 14.2.12.6.4. Out of band signaling in telephone networks has since been provided by a technology known as Signaling System 7 (SS7). *See* ELECTRONIC SURVEILLANCE IN A DIGITAL AGE, *supra* note 93, at 37.

96. *See* HUBER, *supra* note 88, at § 14.2.12.6.4; ELECTRONIC SURVEILLANCE IN A DIGITAL AGE, *supra* note 93, at 39. Making this even more difficult, when effectuating a wiretap, law enforcement must minimize the amount of information not relevant to the purpose of the wiretap that is collected. This requires only intercepting communications expected to be relevant and discontinuing any interception once it becomes apparent that a communication is not clearly relevant. *See*, *e.g.*, Scott v. United States, 436 U.S. 128, 140 (1978).

97. *See* ELECTRONIC SURVEILLANCE IN A DIGITAL AGE, *supra* note 93, at 16, 39; Landau, *supra* note 90, at 16 n.73.

98. *See* ELECTRONIC SURVEILLANCE IN A DIGITAL AGE, *supra* note 93, at 16, 39; Landau, *supra* note 90, at 16 n.73; *see also Scott*, 436 U.S. at 140.

99. H.R. REP. NO. 103-827, at 14–15 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3494–95. *But see* DIFFIE & LANDAU, *supra* note 24, at 219–20 (discussing concerns with the FBI's statistics).

impediments [to lawful wiretaps] posed by new and emerging technologies."[100]

Working around these problems requires giving law enforcement visibility into the routing logic of the phone network; decisions about whether to monitor a given call need to be made whenever the routing of that call changes, not exclusively when the call is initiated. This, in turn, requires engineering telecommunication switches to support that capability.

This situation became even more difficult with the advent of cell phones. The basic operating principle of a cell phone is that it is able to "hop" from one cellular tower to another, in real time, during the course of a conversation. In order to make this work, cellular networks have significantly more complicated routing and switching logic than the landline telephone network. Cellular network switches need to know the specific identity of a phone, which carrier's network that phone is on, and the specific cellular tower (or even multiple towers) that that phone is communicating with.[101] In order to implement a wiretap order involving a call conducted between two phones on a cellular network, that network's switches need to be designed with relevant capabilities.

The Wiretap Act, along with related legislation and jurisprudence, was developed before digitalization of the telecommunications network brought these problems to the fore. Even the 1986 amendments largely failed to appreciate the difficulties that would begin to arise only a few years later. The law was developed for a telecommunications network of circuit-switched "dumb pipes," in which installing a wiretap could be as simple as connecting a pair of jumper cables to the copper wires running to a subject's house.

CALEA was written with the very specific and limited purpose of ensuring that telecommunications carriers would continue to be able to support wiretap orders as they transitioned from "dumb" to "smart" networks.

B. What CALEA Does

CALEA's operative provision requires telecommunications carriers[102] to use telecommunications equipment that implements certain capability requirements.[103] These requirements are relatively

100. H.R. REP. NO. 103-827 at 14, *reprinted in* 1994 U.S.C.C.A.N. 3489, 3494.

101. *See* ELECTRONIC SURVEILLANCE IN A DIGITAL AGE, *supra* note 93, at 18–24, 41–46.

102. The definition of "telecommunications carrier" is discussed below. *See infra* Section III.C, Part IV. For now, it suffices to say that a "telecommunications carrier" is an entity that provides traditional telephone service that allows individuals to place calls to and receive calls from all, or substantially all, public telephone numbers.

103. 47 U.S.C. § 1002(a) (2012). For completeness, it should also be noted that there are civil penalties of $10,000 per day for carriers that are not in compliance with CALEA. 18

straightforward.[104] First, in order to be CALEA-compliant, telecommunications equipment must be able to intercept communications traversing a carrier's network as may be required by a court order.[105] Second, this equipment must be able to provide law enforcement with access to "call-identifying information" (for example, the telephone numbers of both callers and recipients) associated with calls traversing the network.[106] Together, these two requirements effectively require telecommunications carriers to continue being able to implement wiretaps and pen registers.

The third and fourth capabilities required are more mundane. The third requirement is that intercepted communications and call-related information be captured and made available to the government in a standard format and in a manner that allows them to be transmitted to a facility outside of the carrier's premises.[107] And the fourth capability requirement is that the first two requirements be implemented in a way that minimizes interference with the services provided to the carrier's subscribers, does not provide the government with access to more information than that authorized by court order, and maintains the confidentiality of the government surveillance.[108]

The scope and purpose of these capability requirements are narrow. The statutory language, legislative history, and judicial history make clear that the sole purpose of CALEA was to preserve the previous relationship between law enforcement and telecommunications carriers

---

U.S.C. § 2522(c) (2012). There is, however, a safe harbor available if the carrier is using equipment that is compliant with relevant industry standards, 47 U.S.C. § 1006(a)(2) (2012), which may trigger a Federal Communications Commission rulemaking to alter those industry standards in order to ensure compliance. *Id.* § 1006(b). *See also* United States Telecom Ass'n v. Fed. Commc'ns Comm'n, 227 F.3d 450 (D.C. Cir. 2000).

104. While straightforward, each is written to track various statutory and judicial requirements. Exposition of these requirements is not necessary to understand generally how the statute works or to follow the discussion below.

105. 47 U.S.C. § 1002(a)(1) (2012).

106. *Id.* § 1002(a)(2).

107. *Id.* § 1002(a)(3).

108. *Id.* § 1002(a)(4).

and to clarify that relationship insofar as the advent of digital technologies was creating new problems.[109] For this reason, CALEA's substantive requirements apply only to telecommunications carriers.[110] As discussed below, these substantive requirements expressly do not apply to other non-carrier entities, and CALEA does not otherwise alter statutory frameworks or obligations.[111]

Despite its narrow purpose, there are several remarkable things about CALEA's capability requirements. The most apparent thing to note about these requirements is that they maintain the longstanding division between communications and call-identifying information, or content and metadata, established in *New York Telephone Co.*[112] and *Smith*.[113] We see this clearly, as the statute includes separate provisions governing the requirements for communications and call-identifying information. This, however, could merely be a reflection of the different technical requirements needed to implement wiretaps, on the one hand, and pen registers, on the other, in modern digital networks. More notable, however, is that the statute consistently refers to "communications or call-identifying information" — except where it refers to only one category or the other. Perhaps the most important example of the statute referring to only one category is § 1002(b)(3), the encryption limitation. This section, discussed in more depth below, says that telecommunications carriers are under no obligation to decrypt encrypted *communications*. It is notably silent as to the encryption of call-identifying information. As discussed in Part IV, this reflects congressional understandings of the architecture of the telecommunications network,

---

109. H.R. REP. NO. 103-827, at 20 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3500 (stating that the purpose of the legislation is "to define more precisely the assistance that telecommunications carriers are required to provide in connection with court orders"); *id.* at 14, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3494 ("The purpose of the legislation is to further define the [telecommunications] industry duty to cooperate . . . ."); *id.* at 17–18, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3497–98; *id.* at 22, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3502 ("The Committee intends the assistance requirements in section [1002] to be both a floor and a ceiling. The FBI Director testified that the legislation was intended to preserve the status quo . . . ."); *see also United States Telecom Ass'n*, 227 F.3d at 455 ("Because Congress intended CALEA to 'preserve the status quo,' the Act does not alter the existing legal framework for obtaining wiretap and pen register authorization, 'provid[ing] law enforcement no more and no less access to information than it had in the past.'") (alteration in original); *In re* the Application of United States, 441 F. Supp. 2d 816, 819 (S.D. Tex. 2006) ("Congress intended CALEA to preserve the status quo, and therefore the new statute did not modify the legal standards for electronic surveillance via wiretap or pen/trap devices.").

110. Am. Council on Educ. v. Fed. Commc'ns Comm'n, 451 F.3d 226, 228 (D.C. Cir. 2006) ("CALEA applies only to 'telecommunications carrier[s].'") (citing 47 U.S.C. § 1002(a) (1998)) (alteration in original).

111. *See infra* Part IV; *see also United States Telecom Ass'n*, 227 F.3d at 455; *Am. Council on Educ.*, 451 F.3d at 228 ("While CALEA's substantive provisions apply to 'telecommunications carrier[s],' they do not apply to 'information services.'") (citing 47 U.S.C. § 1002(a)–(b) (1998)) (alteration in original); H.R. REP. NO. 103-827, at 17, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3497 (asserting that "information services" are not covered by the bill).

112. United States v. N.Y. Tel. Co., 434 U.S. 159 (1977).

113. Smith v. Maryland, 442 U.S. 735 (1979).

and arguably provides important insights into how Congress may think about encryption on modern networks.

The next remarkable thing about CALEA's capabilities requirements is, frankly, that they exist at all. Congress had not previously imposed prospective burdens on private firms to ensure that they conducted their business or designed their technologies to assist law enforcement, and it was unclear whether the courts would treat existing assistance requirements as requiring firms to undertake such requirements on their own.[114] While firms (and individuals) have had longstanding obligations to provide reasonable assistance to law enforcement under certain circumstances, law enforcement has generally needed to take those providing assistance as they came. If a firm had designed its technology in such a way that frustrated law enforcement efforts, it was unclear whether any recourse was available to law enforcement.[115] CALEA was arguably the first time that Congress had imposed affirmative design requirements on firms in order to support law enforcement capabilities.

Somewhat more subtly, the capabilities requirements are implemented in a way that reflects congressional understandings of how telecommunications networks operate — or, how they operated at the time CALEA was adopted. In particular, Congress understood the telecommunications network to be made up of a centralized network of telecommunications carriers that established transient connections between subscribers. Under this understanding, each subscriber connects to the network through a local telephone exchange (that is, a switch that connects telephone connections between subscribers or other switches). When the calling subscriber dials a number, her exchange routes that call through other inter-connection exchanges to reach the receiving subscriber's exchange, which terminates the call at the receiving subscriber's telephone. These underlying assumptions are seen in part through how the capabilities requirements are implemented. Carriers are not responsible for all communications traversing their networks;

---

114. H.R. REP. NO. 103-827, at 13, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3493 ("[T]he question of whether companies have any obligation to design their systems such that they do not impede law enforcement interception has never been adjudicated."); U.S. CONG., OFFICE OF TECH. ASSESSMENT, ELECTRONIC SURVEILLANCE IN A DIGITAL AGE 2 (1995), https://www.princeton.edu/~ota/disk1/1995/9513/9513.PDF [https://perma.cc/QA69-UEZL]. The Supreme Court in *United States v. New York Telephone Co.* found that 18 U.S.C. § 2518(4) allowed federal courts to compel telecommunication providers to provide "any assistance necessary to accomplish an electronic interception . . ." 434 U.S. at 177. The question of whether a carrier has any obligation to *design* its equipment to facilitate an authorized electronic surveillance under § 2518(4) was never litigated. *See also* Landau, *supra* note 90, at 15 ("[Title III does not] answer the question of whether communication systems equipment and design had to include the ability to perform legally authorized eavesdropping.").

115. *See* Landau, *supra* note 90, at 15.

rather, they are only responsible for communications under their control. If, for instance, a carrier's switch implements a function that allows a call to be redirected to a second carrier's switch, the obligation of intercepting that communication may fall exclusively to the second carrier.[116] This reflects an understanding that every call that enters the network needs to leave it at some point. As such, there will always be at least one ingress or egress point where the call can be intercepted, which yields a consistent location for implementing intercepts. But in order for this to be workable there also needs to be a relatively small number of possible ingress and egress points.

We see this further reflected in the legislative history's discussion of information services and the Internet — the subject of the discussion immediately below.[117] For instance, the House Report briefly discusses the application of CALEA to the Internet, explaining that while CALEA itself does not impose any obligations relating to the Internet, "this does not mean that communications carried over the Internet are immune from interception."[118] Rather, they can be wiretapped like any other electronic communication under the Wiretap Act. Critically, the Report explains that "law enforcement will most likely intercept communications over the Internet at the same place it intercepts other electronic communications: at the carrier that provides access to the public switched network."[119] This reflects an understanding of the Internet modeled on the traditional telephone network, in which individuals connect to the Internet primarily through one of a small number of fixed-line operators — an understanding that is very different from the reality we see today, where individuals freely roam between multiple cellular and (often public) Wi-Fi networks, as well as between devices on these various networks. Perhaps even more jarring is the Report's discussion of e-mail and the relationship between telecommunications carriers and information services in the delivery of e-mail. In one of its more puzzling passages, the House Report explains that "[t]he storage of a message in a voice mail or E-mail 'box' is [an information service, which is] not covered by the bill," but continues by adding that "[t]he redirection of the voice mail message to the 'box' and the transmission of an E-mail message to an enhanced service provider that maintains

116. H.R. REP. NO. 103-827, at 22–23, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3500 (noting that "if an advanced intelligent network directs the communication [from a subscriber's carrier] to a different carrier, the subscriber's carrier only has . . . to ensure that law enforcement can identify the new service provider handling the communication" and also that "a carrier that does not originate or terminate the message, but merely interconnects two other carriers, is not subject to the requirements for the interconnection part of its facilities"); *see also In re* Commc'ns Assistance for Law Enf't Act & Broadband Access & Servs., 19 F.C.C.R. 15676, 15678 (2004) (describing Internet access at the time CALEA was enacted).

117. *Infra* Section III.C.

118. H.R. REP. NO. 103-827, at 23–24, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3503–04.

119. *Id.* at 24, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3504.

the E-mail service are covered."[120] Again, this reflects how Congress thought about the Internet and similar services at the time: there was a core network running over centralized switches operated by a small number of telecommunications carriers, and this network interconnected all of the various users and services on the edges. So long as the core network was made up of CALEA-compliant switches, e-mails traversing the network could be intercepted in the same way as telephone calls. Of course, this is not how the architecture of the Internet has evolved, and as discussed below, the switches that carry the vast majority of content traversing the Internet are not subject to CALEA.[121]

Even though Congress's understanding of how communications networks would evolve over time proved less than prescient, it nonetheless provides useful information about how Congress may think about the same issues today. We will return to this topic in Part V.

C. What CALEA Does Not Do

Despite the fact that CALEA was enacted with a very narrow purpose, it is nonetheless frequently mentioned in discussions of encryption-related law.[122] This is unsurprising given that CALEA featured prominently in the Crypto Wars of the 1990s and has remained a flashpoint for proposed regulation of encryption in the years since. What is more, CALEA has been prominent in conversations about Apple's refusal to assist the FBI in accessing encrypted iPhones.[123] Given the heavy load CALEA is often made to bear in discussions of encryption, it is useful to outline CALEA's limits.

As an initial matter, CALEA does not address encryption.[124] Early drafts of CALEA were intended to address both the need to ensure access to communications and the ability to decrypt any encrypted communications. However, in response to opposition to the bill, Congress and the FBI agreed to bifurcate these issues.[125] As enacted, CALEA's

120. *Id.* at 23, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3503.

121. *See infra* Part IV.

122. For examples of such laws and discussions, see *infra* note 235.

123. For a more extensive discussion about Apple's refusal, see *infra* Part V.

124. In addition to this discussion, see also Section V.B.2, *infra*.

125. *Network Wiretapping Capabilities: Hearing Before the Subcomm. on Telecomms. & Fin. of the H. Comm. on Energy & Commerce*, 103d Cong. 168 (1994) [hereinafter *Network Wiretapping Capabilities Hearing*] (statement of Louis J. Freeh, Director, Fed. Bureau of Investigation) ("The proposal . . . only addresses the technological issue concerning *access to communications* and does not alter the legal requirements currently associated with court-ordered intercepts. With minor exception . . . *the legislation does not address the issue of encryption*." (emphasis added)); *see also id.* ("[T]his legislative proposal focuses only on the issue of interception access within advanced communications networks. The topic of access within advanced telecommunications networks is distinct from encryption and poses an immediate and critical problem for law enforcement for which we are now seeking a legislative solution."); *Network Wiretapping Capabilities Hearing* (letter from William S. Sessions, Director, Fed. Bureau of Investigation, to Honorable Edward J. Markey, Chairman, Subcomm.

capabilities requirements only addressed access to communications.[126] The encryption issue was considered lower priority because the government had developed a new technology — the Escrowed Encryption Standard ("EES") — that it believed would address any immediate concerns.[127] As such, the government planned to return to legislation to address the encryption issue at a later time.[128]

As discussed above, the purpose of CALEA was to preserve the status quo, ensuring that law enforcement continued to have the same wiretapping capabilities on digital telecommunications networks as it had on earlier analog networks. The statute included several provisions narrowing its scope, and its legislative history similarly suggested limitations.

The most important limitation on the scope of CALEA is that its capabilities requirements do not apply to "information services."[129]

---

on Telecomms. & Fin. Of the H. Comm. on Energy & Commerce) [hereinafter Sessions Letter] ("These technologies present a two-fold challenge to law enforcement: first, the ability to access communications . . . and second, the ability to understand intercepted communications on a real-time basis is soon to be defeated by low cost, readily available commercial encryption devices (the encryption issue)."); COMM. TO STUDY NAT'L CRYPTOLOGY POLICY, *supra* note 94, at 216 ("CALEA is not explicitly connected to national cryptography policy . . . ."); *id.* at 225 ("[T]he government chose not to seek legislation outlawing encryption without features for exceptional access, but chose instead to use the [Escrowed Encryption Standard] to influence the marketplace for cryptography."); *id.* at 244 ("[CALEA] calls attention to the relationship between access to a communications stream and government access to the plaintext associated with that digital stream. The former problem must be solved (and was solved, by the CALEA, for telephone communications) before the latter problem is relevant."); DIFFIE & LANDAU, *supra* note 24, at 227.

126. *Network Wiretapping Capabilities Hearing*, *supra* note 125 (statement of Louis J. Freeh, Director, Fed. Bureau of Investigation); COMM. TO STUDY NAT'L CRYPTOLOGY POLICY, *supra* note 94, at 244.

127. *See infra* Section V.B.2; *see also* COMM. TO STUDY NAT'L CRYPTOLOGY POLICY, *supra* note 94, at 224 ("[T]he government chose not to seek legislation outlawing cryptography without features for exceptional access, but chose instead to use the EES to influence the marketplace for cryptography."); DIFFIE & LANDAU, *supra* note 24, at 227; Sessions Letter, *supra* note 125 (noting that "to work towards a balanced, comprehensive national policy concerning the use of encryption with communication devices, the President has recently issued a Presidential Decision Directive regarding the use of a Government-developed key escrow encryption microcircuit called 'Clipper Chip,'" and praising this solution for "achieving an equitable balance between the rights and needs of the American public and business to protect their communications and the legitimate need of law enforcement to conduct court-authorized electronic surveillance").

128. DIFFIE & LANDAU, *supra* note 24, at 227; Letter from Brent Scowcroft to Dick Cheney (Jan. 17, 1992), *in* BRUCE SCHNEIER & DAVID BANISAR, THE ELECTRONIC PRIVACY PAPERS 160 (1997); Memorandum from Brent Scowcroft to the President (Dec. 29, 1991), *in* BRUCE SCHNEIER & DAVID BANISAR, THE ELECTRONIC PRIVACY PAPERS 163 (1997).

129. *See* 47 U.S.C. § 1002(b)(2) (2012) ("The requirements of subsection (a) of this section do not apply to information services . . . .").

Even telecommunications carriers fall within this limitation, to the extent that they are providing information services.[130] Such so-called hybrid services[131] were initially understood by Congress to be the exception but, as is discussed in Parts IV and V, have become the rule. One of the fundamental transitions brought about by the Internet is that today most traditional services provided by telecommunications providers are now provided as information services running over telecommunications services.[132] Similarly, CALEA does not apply to private networks — including those provided by telecommunications carriers.[133]

The legislative history goes further than this, offering discussion both of various types of private networks and of the Internet:

> The only entities required to comply with the functional requirements are telecommunications common carriers, the components of the public switched network where law enforcement agencies have always served most of their surveillance orders . . . .
>
> The bill is clear that telecommunications services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers (these would include long distance carriage) need not meet any . . . wiretap standards. [Private Branch Exchanges] are excluded. So are automated teller machine (ATM) networks and other closed networks. Also excluded from coverage are all information services, such as Internet service providers or services such as Prodigy and America-On-Line.
>
> All of these private network systems or information services can be wiretapped pursuant to court order, and their owners must cooperate when presented with a wiretap order, but these services and systems do not have to be designed so as to comply with the capability requirements. Only telecommunications carriers, as defined in the bill, are required to design and build

130. *See infra* Section IV.A.

131. That is, information services being provided by telecommunications carriers. *See infra* Part IV.

132. The relationship between telecommunications carriers and information services is discussed in Part IV, *infra*.

133. 47 U.S.C. § 1002(b)(2) (2012).

> their switching and transmission systems to comply with the legislated requirements.[134]

There are two noteworthy aspects of this discussion beyond its further emphasis of CALEA's limited scope. First, it is interesting that the legislative history, written in 1994, appears to have recognized — and expressly exempted — Internet Service Providers ("ISP") from CALEA's requirements. That reading of both CALEA and the legislative history, however, is wrong to the extent that one applies it to modern ISPs. It needs to be remembered that, at the time CALEA was drafted, ISPs provided Internet access via dial-up service.[135] One would use a modem to connect to their ISP, via a traditional telephone line provided by a telecommunications network. As will be discussed in Part IV, the statute does apply to services that are "substantial replacements"[136] for telecommunication services, and the Federal Communications Commission ("FCC") has held that some aspects of Internet access service — including the underlying telecommunications component and some services running over top of that component such as fixed voice over Internet Protocol ("VoIP") — are therefore subject to CALEA's capabilities requirements.[137]

Second, CALEA leaves other parts of the ECPA, including the Wiretap and Pen Register Acts, untouched.[138] CALEA imposes obligations upon telecommunications carriers to ensure that Wiretap and Pen Register Act intercepts can still be implemented. However, CALEA says nothing about how these acts apply to other networks. The Wiretap and Pen Register Acts continue to apply to wire and electronic communications regardless of whether they are communicated using networks subject to CALEA's requirements.[139] Indeed, as noted elsewhere in the legislative history, CALEA's capabilities requirements "are in addition to the existing necessary assistance requirements in sections 2518(4) and 3124 of title 18 [parts of the Wiretap and Pen Register Acts], and

---

134. H.R. REP. NO. 103-827, at 18 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3498.

135. *See In re* Commc'ns Assistance for Law Enf't Act & Broadband Access & Servs., 19 F.C.C.R. 15676 (2004) [hereinafter FCC Notice] (FCC notice of proposed rulemaking and declaratory ruling).

136. *See infra* notes 149–151 and accompanying text.

137. *See* FED. COMMC'NS COMM'N, FCC 06-56, SECOND REPORT AND ORDER AND MEMORANDUM OPINION AND ORDER (May 12. 2016), https://apps.fcc.gov/edocs_public/attachmatch/FCC-06-56A1.pdf (last visited May 4, 2017).

138. United States Telecom Ass'n v. Fed. Commc'ns Comm'n, 227 F.3d 450, 455 (D.C. Cir. 2000); *In re* United States, 441 F. Supp. 2d 816, 819 (S.D. Tex. 2006).

139. *See* H.R. REP. NO. 103-827, at 23–24, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3503–04. ("While the bill does not require reengineering of the Internet . . . this does not mean that communications carried over the Internet are immune from interception . . . .").

1805(b) of title 50 [part of the Foreign Intelligence Surveillance Act]."[140]

Similarly, CALEA did not make significant changes to the Stored Communications Act.[141] And it says nothing at all about devices used or controlled by individuals. For instance, individuals are free to use and purchase devices that incorporate otherwise-legal encryption technology, and any government access to those devices is governed primarily by the Fourth and Fifth Amendments.[142] Nothing in ECPA applies to information stored on an individual's device — even if that device is used for communications, or if that information is a communication stored on the individual's own device (as opposed to in electronic storage provided by an electronic communication system). Indeed, CALEA itself does not actually impose any obligations on device and equipment manufacturers, even on those manufacturing telecommunications equipment. Instead, the obligation to use CALEA-compliant equipment is placed on telecommunications carriers, and it is up to these carriers to source and use CALEA-compliant equipment.[143]

IV. CALEA'S LIMITS: HYBRID NETWORKS AND THE CONTINUING DIGITAL (RE)EVOLUTION

While CALEA was meant to be a narrow statute that addressed a specific problem, the network has continued to evolve and the underlying problem has continued to grow since the statute was adopted. CALEA was needed because digitalization of communications allowed control of how communications traversed the network to be pushed from the edge (where it did not interfere with wiretapping capabilities) to switches in the network.[144] In the two decades since, we have transitioned from an almost entirely circuit-switched network (the traditional telephone network) to an almost entirely packet-switched network (the Internet).[145] As a result of this transition, control of how communications traverse the network has swung back to the edges. But this transition has pushed the underlying services to the edge as well. In the

140. *Id.* at 22, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3500; *see also* Sections V.B.2 and V.B.3 (discussing section 2518's assistance requirements).

141. It did eliminate use of administrative subpoenas to obtain "transactional" records about, for example, e-mails, from electronic communications services. H.R. REP. NO. 103-827, at 31–32, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3512. *But see id.* at 23, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3503 (clarifying that information services, such as "[t]he storage of a message in a voice mail or E-mail 'box' [are] not covered by the bill").

142. *See, e.g.*, Timothy A. Wiseman, *Encryption, Forced Decryption, and The Constitution*, 11 I/S: J. L. & POL'Y FOR INFO. SOC'Y 525, 526, 559 (2015).

143. 47 U.S.C. § 1002(a) (2012) (requiring that "a telecommunications carrier shall ensure that its equipment [is compliant]").

144. *See supra* Section III.A.

145. *Id.*

traditional telephone network, the underlying service (voice telephone service) was provisioned by the network. Wiretapping was possible because phone calls had to be transmitted from telephones at the edge to the network core.[146] This is no longer possible today.

This Part discusses the evolution of telecommunications from a service comprising distinct "edge" and "core" functions to a hybridized architecture in which the traditional functions of the edge and core may be intermingled. It starts with a discussion of the clearest example of a hybrid service — voice over Internet Protocol — and considers how CALEA has been applied to this "hybrid" technology. It then considers the limits of such hybrid technologies under CALEA, which offer useful insights into congressional understanding of the structure of communications networks.

A. Early Hybrid Services

As discussed above, the scope of CALEA is limited: it applies only to telecommunications carriers. The purpose of the statute was to preserve the government's ability to effectuate wiretaps of telephone calls, which required the cooperation of only the traditional telecommunications carriers. As defined in the statute, such carriers include "a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire."[147] This definition is meant to encompass a "common carrier that offers wireline or wireless service for hire to the public" and "services or facilities that enable the subscriber to make, receive or direct calls."[148] Moreover, the statute provides the FCC with the power to classify as a telecommunications carrier any other "person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service."[149] This is referred to as the "Substantial Replacement Provision" ("SRP").[150] As explained in the legislative history, "the FCC is authorized to deem other persons and entities to be telecommunications carriers subject to the assistance capability and capacity requirements to the extent that such person or entity serves as a replacement for the local telephone service to a substantial portion of the public within a state."[151]

---

146. *Id.*

147. 47 U.S.C. § 1001(8)(A) (2012).

148. H.R. REP. NO. 103-827, at 20, 23, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3500, 3503.

149. 47 U.S.C. § 1001(8)(B)(ii).

150. *See* FCC Notice, *supra* note 135, at 15697–98.

151. H.R. REP. NO. 103-827, at 20, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3500. The statute provides a three-part test for treatment as a "telecommunications carrier." First, such

CALEA defines a separate class of services, "information services," that are expressly exempted from the statute's substantive provisions. These services are defined as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications."[152] Generally, this category refers to services in which one user connects to another user via the telecommunications network — that is, services being provided by one user on the edge of the network to other users on the edge of the network.[153] The legislative history gives examples of various e-mail and messaging services, but expressly notes its "intention not to limit the definition of 'information services' to such current services, but rather to anticipate the rapid development of advanced software" and that by "including such software-based electronic messaging services within the definition of information services, they are excluded from compliance with the requirements of the bill."[154]

The statute excludes information services from the scope of CALEA in two separate places. In the substantive provisions, the statute expressly states that "[t]he requirements of subsection (a) of this section do not apply to information services."[155] And, as a matter of definition, "[t]he term 'telecommunications carrier' . . . does not include persons or entities insofar as they are engaged in providing information services . . . ."[156]

This statutory structure contains an inherent and substantial ambiguity. The definition of "telecommunications carrier" can be expanded to include entities offering services that can substantially replace the underlying telecommunications service. Such a service could conceivably be offered as an information service — a service that makes available, in real time, voice (or other) information via the underlying telecommunications network. But information services are expressly exempted from the requirements of the Act.

This precise situation developed with the advent of voice over Internet Protocol. VoIP allows users to place "telephone calls" over the Internet. Some of these services are private, meaning that users can call only other users using the same service. Others are more akin to tradi-

---

classification requires "a person or entity engaged in providing wire or electronic communication switching or transmission service . . . ." 47 U.S.C. § 1001(8)(B)(ii). Second, such person or entity is covered only "to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service . . . ." *Id.* Finally, the Commission must also find that "it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of [the] subchapter . . . ." *Id.*

152. 47 U.S.C. § 1001(6)(A).

153. For further discussion, *see infra* Section IV.B.

154. H.R. REP. NO. 103-827, at 21, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3501.

155. 47 U.S.C. § 1002(b)(2) (2012).

156. *Id.* § 1001(8)(C)(i).

tional telephone service, also allowing users to place and receive telephone calls to and from phone numbers on the traditional phone network.

In 2004, the DOJ, FBI, and DEA petitioned the FCC to classify VoIP service as telecommunications services for the purposes of CALEA, such that anyone offering a VoIP service would need to ensure that that service was CALEA-compliant.[157] This led to a rulemaking proceeding in which the FCC held that certain VoIP providers — those offering services that are interconnected with the traditional telephone network — are telecommunications carriers subject to CALEA.[158] This Order was subsequently upheld by the D.C. Circuit Court of Appeals.[159] As explained by the D.C. Circuit:

> To avoid an "irreconcilable tension" between CALEA's [Substantial Replacement Provision] and the information-services exclusion, the Commission concluded that the Act creates three categories of communications services: pure telecommunications (which plainly fall within CALEA), pure information (which plainly fall outside CALEA), and hybrid telecommunications-information services (which are only partially governed by CALEA). The FCC then concluded that broadband and VoIP are hybrid services that contain both "telecommunications" and "information" components.[160]

The Commission went on to find that interconnected VoIP services are substantial replacements for telephone services that include both switching and transmission components, and that classifying them as telecommunications carriers was in the public interest.

The key to understanding the Commission's invocation of "hybrid" services is that CALEA's definitions of telecommunications carriers

---

157. *See* FED. COMMC'NS COMM'N, FCC RM-10865, JOINT PETITION FOR EXPEDITED RULEMAKING iv (2004) (cited and discussed in *In re* Commc'ns Assistance for Law Enf't Act & Broadband Access & Servs., 19 F.C.C.R. 15676 (2004) (FCC notice of proposed rulemaking and declaratory ruling)).

158. *In re* Commc'ns Assistance for Law Enf't Act & Broadband Access & Servs., 20 F.C.C.R. 14989 (2005); *In re* Commc'ns Assistance for Law Enf't Act & Broadband Access & Servs., 19 F.C.C.R. 15676 (2004) (citing FED. COMMC'NS COMM'N, FCC RM-10865, JOINT PETITION FOR EXPEDITED RULEMAKING iv (2004)) (FCC notice of proposed rulemaking and declaratory ruling).

159. Am. Council on Educ. v. Fed. Commc'ns Comm'n, 451 F.3d 226 (D.C. Cir. 2006).

160. *Id.* at 229 (citing *In re* Commc'ns Assistance for Law Enf't Act & Broadband Access & Servs., 20 F.C.C.R. 14989, 14991 (2005)).

and information services are not mutually exclusive.[161] This follows from how information services are excluded from the definition of telecommunications carriers: it excludes "persons or entities *insofar as* they are engaged in providing information services."[162] A telecommunications carrier can, therefore, provide both information services and non-information services, and it will be subject to CALEA only to the extent that it is provided non-information services.

We can think of this in terms of a Venn diagram in which two circles overlap — one for telecommunications carriers and one for information services. The *sine qua non* for CALEA to apply is that one is a telecommunications carrier. If one is a telecommunications carrier, then CALEA applies, to the extent that one is not also providing an information service. In other words, one can be a telecommunications carrier and therefore subject to CALEA's capabilities requirements, while also being exempted from those requirements to the extent that they are also providing an information service. Importantly, this means that there is no such thing as a telecommunications carrier that is not subject to some extent to CALEA's capabilities requirements — if the service that one provides is not to some extent that of a telecommunications carrier, then one is a pure information service and therefore CALEA would not apply to them at all. Where that is the case, one may still be subject to the requirements of the Electronic Communications Privacy Act,[163] but CALEA is entirely inapposite.[164]

B. Hybrid Limits and Centralized, Modular Networks

Interconnected Voice over IP is perhaps the clearest possible example of a hybrid service. It is an information service being used to offer, via telecommunications, the core service offered by telecommunications carriers (voice calling). It is, to use the FCC's language for implementation of CALEA, a "substantial replacement" for voice telephone service in the sense that it can be used to offer the same basic service via a technology deployed as an information service.[165]

Other types of hybrid services are possible — though not all of them will fit into CALEA's rubric for imposing regulatory burdens. For instance, information services offered by a telecommunications carrier

---

161. *Id.* at 234 ("Because CALEA's definitions for 'telecommunications' and 'information service' are not mutually exclusive, the Commission reasonably concluded that mixed services . . . are partially covered by (and partially excluded from) the statute . . . .").

162. 47 U.S.C. § 1001(8)(C)(i) (emphasis added).

163. For a discussion of the Electronic Communications Privacy Act, see *infra* Section V.B.2.

164. *Am. Council on Educ.*, 451 F.3d at 228 ("Because information-service providers are not subject to CALEA, they need not make their networks accessible to law-enforcement agencies.") (citing 47 U.S.C. § 1002(b)(2)(A) (1998)).

165. *See* FCC Notice, *supra* note 135, at 15697–98, 15700–01.

are hybrid services. In this case, the carrier component of the service would be subject to CALEA, but the information service offered via that carriage would not be subject to it. For instance, a telecommunications carrier offering e-mail services would need to employ switches that could intercept e-mails while in transit over their switches, but it would not be under any obligation under CALEA with respect to how those e-mails were stored.[166]

Even more interesting are information services that consumers view as substitutes, but not technological replacements, for core telecommunications services. For instance, instant messaging and video conferencing services like Facebook Messenger, WhatsApp, and Google Hangouts are all clearly information services exempt from CALEA,[167] but they are also substitutes for traditional voice telephone service. Modern information services such as these are a different form of hybrid service. The sort of hybrid services that are covered by CALEA are those in which information services are moving into the network core, either by interconnecting with core telecommunications services (as in the case of interconnected VoIP) or by being hosted by telecommunications carriers. The more interesting and challenging services, however, are those in which traditional telecommunications functionality is moving out of the core. These services are rapidly displacing traditional carrier-based communications services — and, indeed, they are known to be used by parties of interest to law enforcement. The important question is, given that these services offer functionality similar to services traditionally offered by telecommunications carriers, why are they not subject to CALEA?

Understanding why these services are not subject to CALEA tells us something about how Congress was thinking about the structure and operation of communications networks at the time CALEA was adopted. This, in turn, tells us something about the sort of obligations Congress was willing to place on certain parts of the network and why it was willing to do so. Understanding this is helpful for thinking about how Congress may approach modern communications networks.

---

166. *See supra*, note 120. Disclosure of such e-mails would be governed by the Stored Communications Act, 18 U.S.C. §§ 2701–11.

167. *See* H.R. REP. NO. 103-827, at 23 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3503 ("The storage of a message in a voice mail or E-mail 'box' is not covered by the bill. The redirection of the voice mail message to the 'box' and the transmission of an E-mail message to an enhanced service provider that maintains the E-mail service are covered."); *see also In re* Commc'ns Assistance for Law Enf't Act & Broadband Access & Servs., 19 F.C.C.R. 15676, 15706 (2004) (analyzing the legislative history behind CALEA to determine that a "[Local Exchange Carrier] providing the local exchange transmission service that enabled the call to that dial-up ISP — 'the transmission of an E-mail message' — was covered by CALEA as a telecommunications carrier providing . . . [plain old telephone service] functionality" but "the separate ISP was not subject to CALEA because the functions it provided — such as 'the storage of a message in an . . . E-mail "box"' — were 'information services'").

Congressional understanding of the structure of communications networks at the time CALEA was adopted had two key characteristics: these networks were (1) centralized and (2) modular.

At the time CALEA was adopted, communications networks were still overwhelmingly centralized. The vast majority of local telephone service was provided by a monopoly Local Exchange Carrier: the Baby Bells.[168] Cellular service, a nascent market, was overwhelmingly provided by these same carriers.[169] And Internet connectivity was also provided by them. Most of the backbone of the National Science Foundation Network ("NSFNet"), the primary Internet backbone at the time, was provisioned using circuits provided by traditional telecommunications companies.[170] Perhaps more important, NSFNet had a hierarchical structure, following a three-tiered network design.[171] Under this structure, which continued to be used for many years after NSFNet was replaced by a commercial Internet backbone, users accessed the Internet through ISPs[172] They would usually connect to their ISPs via telephone circuits — the same technology that they would use to access other information services of the time, such as CompuServe and Prodigy.[173] These ISPs, in turn, were connected to regional networks by mid-capacity data connections (provided by telecommunications carriers), which were connected to a high-speed nationwide backbone (also

168. It was not until the adoption of the Telecommunications Act of 1996 two years following the adoption of CALEA that the United States fully embraced the idea of promoting competition in local telecommunications markets as opposed to the historical approach of treating these markets as regulated monopolies. The 1984 break-up of AT&T into the Baby Bells, however, had prompted the rapid introduction of new technologies into telecommunications markets, which were increasingly creating challenges for law enforcement. *See, e.g.*, H.R. REP. NO. 103-827, at 14; ELECTRONIC SURVEILLANCE IN A DIGITAL AGE, *supra* note 93, at 2 (discussing effects of transition from a monopoly telecommunications market to a competitive one on wiretapping).

169. *See generally* Erin M. Reilly, *The Telecommunications Industry in 1993: The Year of the Merger*, 2 COMMLAW CONSPECTUS 95, 112 (1994) ("With one half of all cellular licenses originally reserved for the [Regional Bell Operating Companies ("RBOC")], they have been able to invest heavily in cellular services, all seven RBOCs ranking among the nation's ten biggest cellular companies.").

170. KAREN D. FRAZIER, NSFNET: A PARTNERSHIP FOR HIGH-SPEED NETWORKING FINAL REPORT 1987–1995 9 (1995), https://www.merit.edu/wiki/NSFNET_final.pdf [https://perma.cc/4VTJ-FTW2]. The predecessor to NSFNET, ARPANET, had similarly been provisioned over lines leased from AT&T. *See* MITCH WALDROP, DARPA AND THE INTERNET REVOLUTION 80 (2015), http://www.darpa.mil/attachments/(2O15)%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20(Approved).pdf [https://perma.cc/7RGC-J8A3] ("[S]ince nobody was going to give the agency a few billion dollars to string its own wires across the country, ARPA would have to move the data through AT&T's telephone system . . . . [T]he agency would . . . lease [from AT&T] a series of high-capacity phone lines linking one ARPA site to the next.").

171. *See* FRAZIER, *supra* note 170, at 11–12.

172. *See infra* text accompanying note 181.

173. These connections were generally made using modems connected to ordinary telephone lines. In the late 80s and early 90s, there was also a push to deploy Integrated Services Digital Network technology, which was a digital equivalent of a phone line, but it was also provisioned by the local telephone company.

generally made up of connections provided by telecommunications carriers).[174]

In other words, at the time CALEA was adopted, almost all communications went through one of a small number of highly regulated local telecommunications carriers. Congress knew this and structured CALEA around it. No matter whether a person of interest was communicating by landline phone, cellular phone, services such as CompuServe, or Internet-based services such as e-mail, those communications would traverse the local telecommunications carrier's switches. What's more, they would traverse those switches in a common format, making it relatively easy for both the carriers and law enforcement to work with the full range of modes of communications. Knowing this, rather than requiring everyone providing information services to use CALEA-compliant technologies, Congress tailored this obligation to the communications bottlenecks.[175]

Today, it is increasingly the case that the network is not an architectural bottleneck. Most Americans can get wireline telephone (and Internet) service from three or more telecommunications carriers.[176] They can also get cellular telephone (and Internet) service from four or more carriers.[177] Moreover, many have Internet access through an employer, and can readily get online through any of hundreds of Wi-Fi hotspots. Twenty years ago, the vast majority of most Americans' communications was handled by a small number of devices connected to an even smaller number of networks; today, the vast majority of Americans have the ability to seamlessly connect to any number of networks via any number of devices. The architectural bottleneck that existed then, which Congress understood and around which it structured CALEA, is gone today.

Congress also understood the network to be modular. A modular network is one that is made up of several discrete components, each of which performs a discrete set of functions. These modules interconnect

---

174. *See* Rajiv Shah & Jay Kesan, *The Privatization of the Internet's Backbone Network*, 51 J. BROADCASTING & ELECTRONIC MEDIA 93, 94–96 (2007).

175. As explained in the House Report, "[e]arlier digital telephony proposals covered all providers of electronic communications services, which meant every business and institution in the country. That broad approach was not practical." H.R. REP. NO. 103-827, at 18 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3498.

176. *See* FED. COMMC'NS COMM'N, FCC 15-10, 2015 BROADBAND PROGRESS REPORT AND NOTICE OF INQUIRY ON IMMEDIATE ACTION TO ACCELERATE DEPLOYMENT 48 chart 2 (2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-10A1.pdf (last visited May 4, 2017) (showing that 66% of Americans have access to three or more telecommunications carriers offering wireline Internet service).

177. *See* FED. COMMC'NS COMM'N, DA 15-1487, EIGHTEENTH REPORT 14539 chart III.A.1 (2015), https://apps.fcc.gov/edocs_public/attachmatch/DA-15-1487A1_Rcd.pdf (last visited May 4, 2017) (showing that 91.7% of Americans have access to mobile wireless service from four or more carriers).

with one another like pieces in a puzzle to provide some composite service.

In particular, Congress understood that a line could be drawn between telecommunications carriers that provide a telecommunications infrastructure to carry communications between users and between the information and services based upon that information that traverse the telecommunications infrastructure. We see this reflected in part in CALEA's definitions and scope — the bifurcation between telecommunications carriers (subject to CALEA) and information services offered via telecommunications (not subject to CALEA).[178] We also see it reflected in the legislative history. For instance, the House Report, in discussing why CALEA's requirements apply only to telecommunications carriers, notes that law enforcement will generally intercept communications "at the carrier that provides access to the public switched network" — in other words, at the boundary between the information service and the telecommunications carrier.[179] The House Report's discussion of e-mail is also illustrative of Congress's modular understanding of the network; it recognized a functional distinction between providers that offer e-mail services and those that provide for the transmission of e-mails and delineated a difference in legal obligations based on this distinction.[180] As explained by the FCC in its discussion of the legislative history:

> At the time CALEA was enacted, Internet services were generally provided on a dial-up basis by two separate entities providing two different capabilities — a local exchange telephone company carrying the calls between an end user and its chosen Internet Service Provider ("ISP"), and the ISP providing e-mail, content, web hosting and other Internet services. In the *House Report*, Congress was quite clear as to the CALEA status of these different entities: The [Local Exchange Carrier] providing the local exchange transmission service that enabled the call to that dial-up ISP — "the transmission of an E-mail message" — was covered by CALEA as a telecommunications carrier providing a [plain old telephone service ("POTS")] functionality (a "phone call"). By contrast, the separate ISP was not subject to CALEA because the functions it provided — such as "[t]he storage of

178. *See supra* Section IV.A.

179. H.R. REP. NO. 103-827, at 24, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3504.

180. H.R. REP. NO. 103-827, at 23, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3503 (discussing "[t]he storage of a message in a voice mail or E-mail 'box'").

> a message in a[n] . . . E-mail 'box'" — were "information services."[181]

The modularity of the network is particularly important for CALEA, because each module needs to be able to interconnect with other modules. This interconnection requires passing information between each component of the network. Each of those interconnection points is a potential point at which an interception can occur and at which capabilities requirements such as those contained in CALEA can be implemented.

If, however, a service is provided on an integrated, end-to-end, basis — that is, if there is only one "module" that comprises the service and it never needs to hand information to another module — then it can be much harder to effectuate an intercept or to implement capabilities requirements. Importantly, this is largely what is happening with modern "hybrid" services. While these information services continue to rely on telecommunications carriers to carry raw bits of data, all of the logic controlling how those bits of data are processed is being moved from the network core to the edge.

This is the opposite extreme of the problem that necessitated CALEA in the first place. Recall that CALEA was a response to the digitalization of telecommunications switches. As switches became "smart" — as the logic of how calls were routed, placed, transferred, and the like, moved from decisions made and implemented at the edge to decisions made at the edge but implemented at the switch — it became increasingly difficult to intercept communications made over these networks. Today, much of the logic that has historically been part of the telecommunications network is moving to the edge.

The core function of the telecommunications network has always been facilitating voice telephone calls. This requires maintaining databases of phone numbers and ports, maps of the network, routing and billing information, and all sorts of other information needed for the operation of a voice communications network. Today, users accomplish the same "telephone call" using any number of technologies, from e-mail and instant messaging, to social media platforms like Twitter and Facebook Messenger, to Google Hangouts, to fully encrypted communications platforms like WhatsApp. Critically, from the perspective of the telecommunications carrier, all of these services are roughly the same — just a series of bits that the carrier needs to deliver from one user to another. The underlying logic that facilitates these various forms

---

181. *In re* Commc'ns Assistance for Law Enf't Act & Broadband Access & Servs., 19 F.C.C.R. 15676, 15706 (2004) (footnotes omitted) (all but first two alterations in original) (FCC notice of proposed rulemaking and declaratory ruling).

of communication has moved from the network core to the edge — from the carrier to the information service.

V. ASSISTING LAW ENFORCEMENT ACCESS TO ENCRYPTED CONTENT

Communications technology has continued to evolve since CALEA was adopted. Today's communication networks look like nothing imaginable at that time. The Internet is now central to modern life and commerce. It is built on a platform of constant connectivity across myriad carriers, with near-ubiquitous mobile devices. Each of these mobile devices has more storage capacity and computational power than supercomputers had in the early 1990s. Of course, Congress would have great difficulty predicting and accounting for such technology in 1994.

This continued technological development is once again rebalancing the power and burdens between law enforcement seeking to obtain lawful access to information and the rights of individuals to be secure against overbroad intrusion. New technologies are frustrating many efforts by law enforcement to implement their authority under ECPA — though, as discussed below, the greater availability of data generally has also given law enforcement much greater access to information about individuals under investigation. Such increased access comes with its own challenges. First, the relative cornucopia of carriers, and the ease with which users can move between them, makes it much harder to find and intercept the communications of a particular user while the communications are in transit. Second, much information of interest to law enforcement is stored on, or best accessed through applications installed on, the users' devices (for example, smartphones), instead of being intercepted while in transit across a carrier's network. And third, the widespread availability (and, increasingly, use) of strong encryption makes it much harder to access communications or other information either while in transit through a carrier's network or while stored on a device. Each of these challenges is discussed below.

This Part begins with an overview of the ways in which new technologies are affecting the relative balance between the rights of individuals and law enforcement's need to access their information. It then considers what lessons we can learn from CALEA about how Congress may generally respond to these changes.

A. What's Going On?

Current tensions between the needs of law enforcement to access, and the rights of individuals to be reasonably secure in, electronic communications are the result of a number of technological trends that have

been ongoing for nearly three decades. The precursor to all of these trends was the development of the transistor, which led to both digitalization of information and the advent of the modern computer. But the most important contemporary developments were almost certainly the introduction of the Apple iPhone in 2007 and the Apple App Store in 2008.

1. What the iPhone Wrought

The communications landscape was already undergoing substantial evolutionary change even prior to the introduction of the iPhone in 2007. Internet usage was drastically expanding.[182] The number of telecommunications carriers available to most consumers had increased dramatically from the local telephone monopolies that existed in 1994.[183] There had also been a massive shift underway from landline telephones to mobile phones.[184] Each of these trends has made it incrementally more difficult for law enforcement to obtain access to communications. And, as discussed above, law enforcement and the FCC tailored the application of CALEA to the changing technologies on the ground, to the extent permitted by the bounds of the statutory framework.[185]

But the iPhone represented a revolutionary change to the telecommunications landscape. When it was introduced in 2007, the iPhone was the first device that was as much a small computer as it was a phone. Prior to the iPhone, landlines and mobile telephones connected to the telephone network and computers connected to the Internet (sometimes via the telephone network). Phones were for accessing the telecommunications services provided by telecommunications carriers;

---

182. *See* WIRELINE COMPETITION BUREAU, HIGH-SPEED SERVICES FOR INTERNET ACCESS: STATUS AS OF DECEMBER 31, 2007, at chart 5 (2009), https://apps.fcc.gov/edocs_public/attachmatch/DOC-287962A1.pdf (last visited May 4, 2017) (showing growth in residential high-speed Internet connections from 3.9 million in 2000 to 80 million in 2007).

183. *See* WIRELINE COMPETITION BUREAU, LOCAL TELEPHONE COMPETITION: STATUS AS OF JUNE 30, 2007, at tbl. 16 (2008), https://apps.fcc.gov/edocs_public/attachmatch/DOC-280943A1.pdf (last visited May 4, 2017).

184. The number of residential landlines in the United States has fallen from a peak of about 145 million in June of 2000, WIRELINE COMPETITION BUREAU, *supra* note 183, to 77 million in June of 2013, WIRELINE COMPETITION BUREAU, LOCAL TELEPHONE COMPETITION: STATUS AS OF JUNE 30, 2013, at fig.1 (2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-327830A1.pdf [https://perma.cc/L6MJ-HB3E]. In that same timeframe, the number of mobile wireless subscribers in the United States has grown from about 100 million, FED. COMMC'NS COMM'N, COMMERCIAL MOBILE RADIO SERVICES (CMRS) COMPETITION REPORT (6TH ANNUAL) 5, https://apps.fcc.gov/edocs_public/attachmatch/FCC-01-192A1.pdf [https://perma.cc/FMZ7-PDV7], to about 330 million, FED. COMMC'NS COMM'N, COMMERCIAL MOBILE RADIO SERVICES (CMRS) COMPETITION REPORT (19TH ANNUAL) 10542 chart II.B.1, https://apps.fcc.gov/edocs_public/attachmatch/FCC-01-192A1.pdf [https://perma.cc/G5VJ-YLZ4].

185. *See* Am. Council on Educ. v. Fed. Commc'ns Comm'n, 451 F.3d 226 (D.C. Cir. 2006).

computers were for accessing information services. Both could be used for communicating with others, but using different paradigms: phones were used for phone calls and text messages; computers were used for e-mail and instant messaging. The iPhone merged these two platforms. And it did so in a mobile form factor, meaning that it was a computer that could always be with its user. This transition from mobile phone to mobile computer was completed with the introduction of the App Store the following year. The App Store allowed users to develop and run their own software on their iPhones, effectively completing the iPhone's transition from a mere phone to a general-purpose computing device.

Once the phone and computer were merged into a single platform it was only a matter of time before the communications facilitated by telecommunications and information services would also be merged. From the user's perspective, there is little difference between the two, especially as "information services" increasingly offered VoIP (or even video conferencing) functionality and as text messaging gave way to other, less expensive services for sending short messages in text form. The only real difference between these services is where the computational logic that makes them work is located — in the telecommunications carrier's network (for telecommunications services) or on the user's device (for information services).

2. Widespread Encryption

The next step along the path to where we are today was the widespread deployment of encryption, first for communications between users' phones and Internet-based services and, more recently, for the content on the devices themselves.[186]

Soon after the advent of the World Wide Web, protocols were developed to allow for encrypted communications between web browsers and servers.[187] The first of these protocols, SSL 2.0, commonly known

186. For a background discussion of encryption, see *supra* note 60.

187. This discussion of encrypted communications focuses on encrypted web traffic, which was first introduced publicly in 1995. There are, of course, many other forms of encrypted communications. The encrypted phones being developed by AT&T in the early 1990s, for instance, implemented very similar encryption technologies. *See infra* Section V.B.1. Research was underway to develop other encrypted Internet-based communications protocols at roughly the same time. The first version of Secure Shell, for instance, was first introduced in 1995. *See* DAVID J. BARRETT, RICHARD E. SILVERMAN & ROBERT G. BYRNES, SSH, THE SECURE SHELL: THE DEFINITIVE GUIDE 9–10 (O'Reilly Media, Inc. 2005). It is no coincidence that these various communications technologies — all of which are information services — were incorporating encryption at the time; they all grew largely out of similar research and concerns about the security of communications. These concerns were particularly important for the Internet, which was in the midst of a transition from an academic and government research network to a commercial network and platform for e-commerce.

as "HTTPS," was publicly released in 1995.[188] These protocols were developed largely in response to concerns that unencrypted information could easily be intercepted on the Internet, both by law enforcement with legal authorization and by any number of other, potentially nefarious, third parties. These concerns were particularly important on a prospective basis, recognizing the Internet's potential as a platform for commerce and the concomitant need to keep information such as financial transactions secure.

Importantly, this encryption served two distinct purposes: confidentiality and authentication. Confidentiality refers to the inability of eavesdropping third parties to read intercepted communications. This is the most commonly understood function of encryption: it turns a message between two parties into gibberish that only those two parties can make sense of, such that they don't need to worry about whether the message is intercepted. Authentication is just as, and arguably more, important than confidentiality. Authentication means confirming that the person (or website) that you are communicating with is, in fact, the entity that you believe it to be. This is particularly important on the Internet: without authentication, for instance, your web browser has no way of ensuring that a website you are attempting to access is the real website or a fake one — that is, whether the website that you reach when you go to http://www.apple.com/ is really Apple's web site or a clever forgery. There are many ways, for instance, of redirecting a web browser from a bank's real website to a fake website that is designed to steal your account information.[189] Encryption can be used to confirm the identity of web servers, such that you can be confident that the website with which you are communicating is the one that it purports to be.

The development of device-level encryption is a more recent phenomenon — one that has been driven by the widespread adoption of mobile phones.[190] It is also something that has been proceeding incrementally. There are different approaches to encrypting devices, and these technologies have been deployed and adopted to varying degrees.

---

188. *See* Kipp E.B. Hickman, *The SSL Protocol*, IETF DRAFT STANDARD (Apr. 1995), https://tools.ietf.org/html/draft-hickman-netscape-ssl-00 [https://perma.cc/7FTP-QJLL].

189. The prototypical implementation of this sort of attack is the "man-in-the-middle" attack. *See* Bruce Schneier, *Man-in-the-Middle Attacks*, SCHNEIER ON SECURITY (July 15, 2008, 6:47 AM), https://www.schneier.com/blog/archives/2008/07/maninthemiddle_1.html [https://perma.cc/F29S-YVV5]. Generally, an attacking computer is able to redirect communications sent by a user (the client) intended for one server (the host) to another server (the "man in the middle"). The man in the middle records the client's communications and then sends them on to the intended host, pretending to be the client. The host's responses are then sent back to the man in the middle, which again records them and sends them along to the client, this time pretending to be the host. From both the client's and host's perspectives, the communications channel seems to be operating as intended.

190. Software that fully encrypts users' hard drives has been commercially available since at least the early 1990s. More recently, hardware-based disk encryption is increasingly available. These technologies, however, have never been widely adopted by ordinary computer users.

Indeed, until the release of the recent iPhone model, strong full-device encryption was the exception, but today it is increasingly the norm. This form of encryption is concerned with preventing access to information stored on a device in the event of its loss or theft. This concern is in many ways more pressing than that of intercepting communications: modern smartphones store unprecedented amounts of information about us.[191] Access to someone's smartphone can easily provide access to all of that individual's communications and contacts, a record of their whereabouts, records of (and access to) websites they have visited, and potentially even access to their financial information, along with much other information.

3. Encryption and Law Enforcement

The widespread availability of encryption has been a continual thorn in the side of law enforcement. Early versions of what became CALEA would have banned the use of encryption in communications outright — at least, the use of encryption that the government couldn't trivially reverse.[192] And in the years since, the FBI has repeatedly sought legislation that would limit the use of encryption both for communications and on devices.[193] To date, none of these efforts have been

191. Riley v. California, 134 S. Ct. 2473, 2485 (2014) ("Cell phones . . . place vast quantities of personal information literally in the hands of individuals."); *see also id.* at 2491 ("[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house . . . .") (emphasis in original).

192. *See infra* Section V.B.

193. There was a great deal of attempted legislative activity relating to encryption in 1997. A draft Electronic Data Security Act, which would have required lawful government access to encrypted communications, was drafted but not introduced early in the year. *See infra*, note 235. Two other pieces of legislation were introduced in 1997, both with the purpose of liberalizing encryption policy in the United States; however, both were ultimately replaced or amended with language that would encourage or require key escrow. In the Senate, the "PROCODE" Act was replaced with the Secure Public Networks Act, which would have encouraged organizations to use key escrow. Similarly, in the House, the Security and Freedom Through Encryption (SAFE) Act, which initially included strong language protecting individuals' ability to use encryption, was amended to require mandatory key escrow. *See* SHARON K. BLACK, TELECOMMUNICATIONS LAW IN THE INTERNET AGE 377 (Morgan Kaufmann 2001); Catherine M. Horiuchi, *Case Study of H.R. 695: The Security and Freedom Through Encryption (SAFE) Act* 12 (NAT'L INST. STANDARDS TECH. 1998), http://csrc.nist.gov/nissc/1998/proceedings/paperG5.pdf [https://perma.cc/U9PU-3H6T] (discussing amendments to the SAFE Act, including FBI Director Freeh's advocacy). Further efforts to legislatively limit the use of encryption have periodically arisen. *See*, *e.g.*, Michael Vatis & Daniel Mah, *FBI's "Super-CALEA" Proposal: More Devices Covered, More Burdens on Industry*, STEPTOE & JOHNSON LLP (Aug. 9, 2006), http://www.steptoe.com/publications-2791.html [https://perma.cc/5UYE-PHHH]; Charlie Savage, *Officials Push to Bolster Law on Wiretapping*, N.Y. TIMES (Oct. 18, 2010), http://www.nytimes.com/2010/10/19/us/19wiretap.html [https://perma.cc/8DMZ-TDMW]; Charlie Savage, *U.S. Weighs Wide Overhaul of Wiretap Laws*, N.Y. TIMES (May 7, 2013), http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html [https://perma.cc/G5NX-QWU6].

successful, for reasons discussed below.[194] But it is likely that the widespread adoption of strong device and end-to-end encryption will force renewed congressional consideration of the issue.[195]

The FBI refers to the challenges created for it by encryption as "going dark."[196] This refers to the FBI's inability to "see into" encrypted communications and devices. Absent technical roadblocks (and, most significantly, encryption), the FBI and other law enforcement can effectuate wiretaps under Title III (the Wiretap Act), access data stored on remote servers under Title II (the Stored Communications Act), and access information stored on an individual's own devices with a warrant issued pursuant to the Fourth Amendment. As encryption becomes increasingly widespread, law enforcement incrementally loses each of these abilities.

It should be noted that there is an offsetting effect, sometimes characterized by the argument that we are in a "golden age for surveillance."[197] While law enforcement is losing access to much of the investigative information that it has traditionally sought, it (along with non-law enforcement entities) is also gaining access to troves of new information.[198] New technologies, for instance, that recognize license plates and even faces have the potential to allow ubiquitous tracking of individuals.[199] Cell phones leave traces as they move from one tower to another, leaving another way to track individuals' movements.[200] Almost every website you visit leaves a record, which law enforcement may be able to detect.[201] And there are myriad other fingerprints and

194. *See infra* Section V.B.

195. *See infra* Part VI.

196. *See*, *e.g.*, James B. Comey, Director, Fed. Bureau of Investigation, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014), *available at* https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [https://perma.cc/TNP5-9Q7K]; *see also Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 10 (2011) (statement of Valerie Caproni, General Counsel, Federal Bureau of Investigation), *available at* https://archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies [https://perma.cc/LK3G-CMUZ].

197. Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 466 (2012).

198. *Id.*

199. *See* Shaun Spencer, *Data Aggregation and the Fourth Amendment*, 19 NO. 4 J. INTERNET L. 13, 15–16 (2015); *see also* Roger Ford, *Unilateral Invasions of Privacy*, 91 NOTRE DAME L. REV. 1075, 1083–84, 1099 (2016).

200. *See* Nathaniel Wackmaw, *Historical Cellular Location Information and the Fourth Amendment*, 2015 U. ILL. L. REV. 263, 269–72 (2015).

201. *See*, *e.g.*, Peter Swire et al., *Online Privacy and ISPS* 8 (Feb. 29, 2016) (unpublished working paper), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf [https://perma.cc/G2TC-EWQE] (discussing the range of data collected by various types of websites).

breadcrumbs that we are constantly leaving behind in our modern technology-infused lives — all of which provide new sources of information for law enforcement.[202]

The challenge with the going dark arguments, as well as their inverse "going bright" counterarguments, is that the information gained from going bright doesn't necessarily correspond to that lost from going dark. Different types of information are needed for different types of investigations, and different law enforcement agencies and activities are affected differently and to varying extents by the changes being brought about by modern communications technologies. What is more, these changes are ongoing, and over time they are unlikely to favor law enforcement. Every day an increasing volume of Internet traffic is encrypted, and more devices are supporting device-level and end-to-end encryption.[203] The tech and activist communities view securing communications and devices as a priority, so new technologies are constantly being developed and deployed that will further exacerbate the going dark concern. At the same time, current laws that make going bright possible are likely at their nadir. Today's understanding of the Fourth Amendment effectively gives law enforcement access to and the right to use nearly any information that can be collected about an individual from third-party sources or while they are in public spaces.[204] It is hard to imagine this legal regime being any more permissive. It is rather more likely that the law will change to limit law enforcement access to this sort of information, which would reduce the extent to which things are going bright.

In terms of who is affected by law enforcement access to stored and in-transit communications, there are three particular categories of individuals that should be considered separately in order to understand the effects of encryption. The first category is those deemed to be potential threats to national security. Today, this is probably the highest profile justification raised by law enforcement to substantiate concerns about going dark. Stated starkly, the concern is that terrorists are using encrypted communications platforms, limiting the government's ability to identify, prevent, and respond to terrorist activities. And the reality is that terrorists *are* using encryption to avoid detection, though the extent of this use and the extent to which it limits law enforcement's ability to act against terrorism are debatable.[205]

---

202. *See Don't Panic: Making Progress on the "Going Dark" Debate*, HARV. BERKMAN CTR. FOR INTERNET & SOCIETY 3 (2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/CCU6-52CD].

203. *See id.* at 28–30.

204. This is a function of the third-party doctrine. *See supra* Section II.A; *see generally* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 574 (2009).

205. *See, e.g.,* Robert Graham, *How Terrorists Use Encryption*, CTC SENTINEL (June 16, 2016), https://www.ctc.usma.edu/posts/how-terrorists-use-encryption [https://perma.cc/

The second category is dissident, minority, and persecuted groups of individuals — especially those in repressive regimes where the government is likely to monitor communications in order to silence and take action against dissent. These groups often rely on encrypted communications to protect themselves from supposed "law enforcement" efforts to suppress their voices or activities.[206] Just as concerns relating to terrorism are the highest-profile argument for the government's need to be able to access encrypted communications, concern about protecting persecuted individuals and groups from oppressive governments is the highest-profile argument for encryption advocates and researchers.

The third category of people affected is lower profile, but arguably most important: those under ordinary criminal investigations. There are thousands of instances in which law enforcement needs to access potentially encrypted communications every year, the majority of which do not relate to national security investigations.[207] Police departments around the country seek to access hundreds of phones every month as part of routine investigations.[208] Information stored on phones is central to investigations ranging from traffic accidents to theft, white collar crimes, assaults, and homicides. While concerns relating to preventing terrorism and promoting democratic values in hostile regimes draw the most headlines, the effect of encryption is likely greatest on common, every-day investigations. This is particularly the case given the relative sophistication of the parties. Both terrorists and dissidents are relatively sophisticated parties who have an incentive and ability to hide their communications from the government. Even if encryption software was outlawed, the underlying algorithms are already understood and widely available. We can easily imagine these actors finding ways to make use of strong encryption to hide their respective activities from government surveillance, independent of local legal barriers. The ordinary criminal, on the other hand, is far less likely to have the incentive, foresight, or ability to make use of these technologies.

JZE4-X7EZ]; Sebastian Rotella, *ISIS via WhatsApp: 'Blow Yourself Up, O Lion'*, PROPUBLICA (July 11, 2016, 7:00 AM), https://www.propublica.org/article/isis-via-whatsapp-blow-yourself-up-o-lion [https://perma.cc/B8PP-SC2C].

206. *See, e.g.*, *On the Use of Encryption and Anonymity in Digital Communications*, HUMAN RIGHTS WATCH (Feb. 2015), https://www.hrw.org/sites/default/files/related_material/EncryptionandAnonymity_Feb1015.pdf [https://perma.cc/D362-L2FD].

207. *See*, *e.g.*, Chris Strohm, *FBI's Comey Says 'You're Stuck with Me' for Another Six Years*, BLOOMBERG POLITICS (Mar. 8, 2017, 11:08 AM), https://www.bloomberg.com/politics/articles/2017-03-08/fbi-s-comey-says-you-re-stuck-with-me-for-another-six-years [https://perma.cc/2DSU-6MR3] (quoting FBI Director James Comey's statement that "[f]rom October to December 2016, about 1,200 of 2,800 devices seized by law enforcement couldn't be accessed by FBI personnel due to encryption"); *see also Report on Government Information Requests*, APPLE (Oct. 4, 2016), http://images.apple.com/legal/privacy/transparency/requests-2016-H1-en.pdf [https://perma.cc/GX9P-JL96] (documenting 4822 requests from U.S. law enforcement for assistance relating to an Apple device and another 1363 requests for assistance accessing an Apple user's account in the first half of 2016).

208. *See Report on Government Information Requests, supra* note 207.

4. Apple, Encryption, and Law Enforcement

All of these issues came together in the fight between Apple and the FBI over access to the iPhone used by Syed Farook, one of the "San Bernardino Shooters." On December 2, 2015, Farook, an employee of the San Bernardino County Department of Public Health, along with his wife, attacked the Department's annual Christmas Party, murdering fourteen people and injuring twenty-two others.[209] They then fled by vehicle and were killed in a confrontation with police. Subsequent investigation determined that the couple had ties to terrorist organizations. In response to this attack, the FBI sought to obtain access to sources of information that might shed light on Farook's potential ties to terrorist organizations.[210]

One source of information to which the FBI sought access was Farook's iPhone 5C.[211] Unfortunately, this model of phone included both device-level encryption and protection features that interfered with the FBI's ability to attempt to circumvent that encryption[212] — any attempt to circumvent the encryption risked deleting all of the information on the device.[213] Unable to access the contents of the device, the FBI sought, and initially received, an order to compel Apple to assist in developing a way to bypass the iPhone's protection features.[214] This order allowed Apple to seek a hearing to challenge it, which Apple promptly did.[215] The order also prompted critical responses from many

209. For a general background on the San Bernardino shooting, see Steven R. Morrison, *Breaking iPhones under CALEA and the All Writs Act: Why the Government Was (Mostly) Right*, CARD. L. REV. (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2808773 [https://perma.cc/ZSW2-XMXZ].

210. *Id.*

211. This phone was owned by Farook's employer, who had consented to allowing the government to access it. Government's Motion to Compel Apple Inc. to Comply With This Court's February 16, 2016 Order Compelling Assistance in Search; Exhibit No. 5:16-CM-00010-SP at 6, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 5:16-cm-00010-SP (C.D. Cal. Feb. 19, 2016) [hereinafter Government's Motion to Compel Apple Inc.] (noting that "the owner of the iPhone, Farook's employer, also gave the FBI its consent to the search").

212. For a discussion of the encryption protecting Apple's iPhone devices, see *infra* note 269.

213. More precisely, the iPhone 5C incorporates features that delete certain of the decryption keys that the device uses to access information stored on it if a user incorrectly enters the device PIN too many times. While this does not "delete" the information stored on the device, it has the same effect, making the information nearly impossible to recover.

214. *See* Government's Motion to Compel Apple Inc., *supra* note 211, at 6.

215. Apple CEO Tim Cook announced Apple's intent to challenge the order in a public letter posted to Apple's website on February 16, 2016. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter [https://perma.cc/4MYV-YK8J]. Apple filed its motion to vacate the order on February 25, 2016. Apple Inc's Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance, *In re* Search of an Apple iPhone Seized During the

in the technical and civil liberties communities.[216] Shortly before the scheduled hearing, the FBI informed the court that it was exploring a newly identified approach to obtaining access to the device without Apple's assistance.[217] The hearing was delayed and, one week later, the FBI informed the court that it had successfully obtained access to the device and withdrew its request for an order compelling Apple's assistance.[218]

From academic and press coverage to legal filings and congressional testimony, much of the discussion about the conflict between Apple and the FBI has focused on CALEA; however, the reality is that CALEA is arguably unrelated to this case, insofar as the case is about access to information stored on a device that is neither manufactured for nor used by telecommunications carriers. The obligations imposed by CALEA fall only upon telecommunications carriers, and they relate only to the interception of information in transit.[219]

At the same time, the central question in this case is whether the government can compel the designers of communications platforms and devices to design their devices in ways that assist in obtaining information from those platforms. CALEA is a remarkable statute precisely because it required telecommunications carriers to prospectively design their networks so that such assistance could be rendered.[220] CALEA imposed this requirement narrowly, carving out various broad exemptions — including for information services and encryption. It is unclear, however, what those exemptions mean for the Apple case. On the one hand, one can infer from CALEA that Congress is comfortable with courts broadly compelling such assistance, in the absence of a particular statutory exemption. On the other hand, one could argue that CALEA demonstrates specific statutory authority is needed in order to compel such assistance, and that CALEA's narrow structure and exemptions demonstrate that the scope of such assistance should be limited.

Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 5:16-cm-00010-SP (C.D. Cal. Feb. 19, 2016).

216. The many briefs filed in support of Apple are collected in Morrison, *supra* note 209. A number of briefs were also submitted in support of the government. In the interest of disclosure, I co-authored a brief in support of neither side, which was ultimately not docketed in the case.

217. *See* Morrison, *supra* note 209.

218. Devlin Barrett & Daisuke Wakabayashi, *FBI Opens San Bernardino Shooter's iPhone; U.S. Drops Demand on Apple*, WALL ST. J. (Mar. 28, 2016, 10:20 PM), http://www.wsj.com/articles/fbi-unlocks-terrorists-iphone-without-apples-help-1459202353 [https://perma.cc/53AL-4ANB].

219. *See supra* Section III.B.

220. In a sense, CALEA answers the question whether carriers can design technologies that frustrate law enforcement; the very genesis of CALEA was in response to the carriers having inadvertently done just that. *See supra* notes 114–116.

At this point, these questions are unlikely to be resolved in court in the near term. There are no currently pending cases in which the FBI is seeking such assistance and, after the dispute over the San Bernardino iPhone, it seems unlikely that the FBI has the appetite to pursue these issues in litigation — especially given the resistance it faced there, in a case that presented incredibly favorable facts for the FBI's position. Rather, this discussion has moved to the legislative arena.

B. What Can We Learn from CALEA?

Even though CALEA is not directly relevant to the Apple case, it has been thrust into the spotlight as providing guidance as to whether firms should be permitted to develop and market products and services to which law enforcement cannot obtain access. It is unsurprising that CALEA is being used for this purpose — CALEA itself arose out of the earlier Crypto Wars and, since that time, it has been central to arguments for both more and less regulation of encryption.

1. CALEA and Encryption

Before proceeding, it is important to recognize a shift in the discussion. Both CALEA and the Apple case are not technically about encryption — they are about the assistance that providers of communications platforms are required to give law enforcement in accessing encrypted communications. However, the contemporary discussion focuses almost entirely on encryption because encryption is the primary obstacle facing law enforcement today in its efforts to access information. Once law enforcement agencies have access to a device, especially a mass-market or consumer-oriented device, they generally can obtain access to the raw data stored on the device without great difficulty. The challenge comes if that data is encrypted — if it is, it can be effectively impossible to decrypt that data into usable form. This is the central difference between the problem that CALEA was meant to address and the modern problem. At the time of CALEA's adoption, a decision was made to bifurcate the issues of access to communications and decryption of those communications.[221] The access issue was more pressing at the time, so CALEA was written to address only that, deferring concerns about encryption to future legislation.[222] CALEA was needed because digital switching was making it difficult for law enforcement to intercept communications traversing telecommunications networks, encrypted or not (primarily transient voice communications,

221. For discussion of the bifurcation between *access* to communications and *decryption* of the contents of those communications, see Section II.B, *supra*.

222. *See supra* Section II.C.

which would be lost if not contemporaneously recorded).[223] In the modern setting, law enforcement can often obtain data stored on a device but may need assistance to decrypt it into usable form.

Legislative consideration of decryption assistance obligations was found in predecessors to CALEA, which would have prohibited telecommunications carriers from carrying traffic that they are unable to decrypt in response to a court order.[224] The background of such proposed requirements is important to understand. At the time CALEA was being considered, AT&T was developing an end-to-end encrypted telephone product, the TSD-3600.[225] Any two individuals who had these phones would be able to activate an encrypted communications mode that would effectively prevent anyone from intercepting the unencrypted contents of the call. In response, the government sought to do two things. First, in CALEA (and the earlier legislation that ultimately became CALEA), Congress would have prohibited encrypted communications devices and services that didn't also have a "backdoor" — a way for lawfully authorized law enforcement to obtain access to the underlying unencrypted communications.[226] And second, the government developed a new "escrowed encryption standard" to implement such a backdoor.[227] Introduced in 1993, EES was an encryption protocol designed to facilitate law enforcement decryption of communications by using a system of multiple keys, some of which would remain in law enforcement control. The government incorporated the EES protocol into a low-cost, commercially available microchip that could be added into commercial electronics. This microchip was called the "Clipper Chip."[228]

Neither of these efforts proved successful. In response to concerns from technology and civil liberties groups, the FBI backed down from its efforts to obtain a statutory ban on the use of non-backdoored communication devices. Rather, the FBI's efforts bifurcated to focus on

---

223. *See supra* Section II.A.

224. In 1991, for instance, then-Senator Biden proposed legislation that would have required carriers to decrypt communications carried over their networks. *See* Comprehensive Counter-Terrorism Act of 1991, S. 266, 102nd Cong. (1991) ("It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law.").

225. *See* DIFFIE & LANDAU, *supra* note 24, at 232–34 (discussing the origins of the TSD as starting in 1991); *see also* Letter from William S. Sessions to George J. Tenet (Feb. 9, 1993) (on file with the Electronic Privacy Information Center).

226. *See*, *e.g.*, *supra* note 224; *see also* DIFFIE & LANDAU, *supra* note 24, at 205–06, 231.

227. *See* DIFFIE & LANDAU, *supra* note 24, at 234–36 (discussing the EES); *see generally* COMM. TO STUDY NAT'L CRYPTOLOGY POLICY, *supra* note 94, at 167–69 (same).

228. *See* DIFFIE & LANDAU, *supra* note 24, at 236–39; *see also* COMM. TO STUDY NAT'L CRYPTOLOGY POLICY, *supra* note 94, at 167–69; Letter from William S. Sessions to George J. Tenet, *supra* note 225.

separate "access" and "encryption" issues.[229] The focus in CALEA was narrowed to address the then-pressing concern that digital telephony was hindering law enforcement access to communications.[230] On the encryption issue, it was the FBI's belief that government adoption of EES would lead to standardization and widespread public adoption of the technology, addressing the separate encryption problem.[231] As such, instead of banning such devices and services, the final version of CALEA expressly allows the use of such devices and services on telecommunications networks.[232]

Unfortunately for law enforcement, the Clipper Chip fell on embarrassing and hard times when it was shown to have significant design flaws that rendered it insecure.[233] As a result, it failed to gain any significant traction, and the FBI's stratagem proved to be for naught. To the contrary, the failures of the Clipper Chip demonstrate a fundamental difficulty with implementing encryption: it is very hard to do well. Indeed, one of the enduring lessons from the failure of the Clipper Chip is that it is hard to properly implement encryption between two parties — designing and implementing a system that allows for decryption by a third party adds substantial complexity that is exceptionally difficult to overcome.[234]

2. Lessons from CALEA

As a result of this complex history, taking lessons from CALEA about encryption is a fraught endeavor. The FBI believed that it had a

---

229. *See supra* Section II.C.

230. *Id.*

231. *See* COMM. TO STUDY NAT'L CRYPTOLOGY POLICY, *supra* note 94, at 225 (describing the government's hope that its own adoption of EES "would lead to a significant demand for EES-compliant devices, thus . . . making EES-complaint devices more attractive [for] other uses" and how the government later "persuaded AT&T in 1992 to base a secure telephone on the EES").

232. 47 U.S.C. § 1002(b)(3) (2012); *see also* H.R. REP. NO. 103-827, at 22 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3504 ("[T]elecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court-ordered wiretaps, unless the carrier provided the encryption and can decrypt it[,] consistent with the obligation to furnish all necessary assistance under 18 U.S.C. Section 2518(4)."). The legislative history notes that CALEA specifically did not "prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access." H.R. REP. NO. 103-827, at 22, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3504. In addition, CALEA was not intended to "address the 'Clipper Chip' or Key Escrow Encryption issue, . . . limit or otherwise prevent the use of any type of encryption within the United States[, or] . . . be in any way a precursor to any kind of ban or limitation on encryption technology." *Id.* In fact, the CALEA had a provision specifically to "protect[] the right to use encryption." *Id.*

233. Blaze, *supra* note 73, at 59.

234. ANDERSON, *supra* note 62, at 794 ("One of the engineering lessons from this whole process is that doing key escrow properly is hard. Making two-party security protocols into three-party protocols increases the complexity and the risk of serious design errors, and centralizing the escrow databases creates huge targets.").

workable escrow standard that mooted the need to address encryption at the time CALEA was adopted. Congress and the FBI very deliberately did not address encryption in the statute, so it is factually wrong to say that CALEA addressed encryption in any direct or meaningful way — let alone that it is a blanket expression of congressional approval for the use of encryption. The language in the statute and legislative history were meant to say that CALEA did nothing to affect the then-existent technologies, not to give carte blanche to future technologies. On the other hand, this result was itself a retrenchment of the FBI's initial efforts to place limits on the use of encryption. And it was only the first of several such failed efforts by the FBI; in the years since, the FBI has frequently sought to expand the scope of CALEA to limit the use of encryption and each time has failed.[235] It is, of course, a mistake to interpret failure to adopt legislation as indication of congressional intent. Indeed, legislation that would affirm and protect the use of strong encryption has also failed.[236] Really, the only thing that CALEA can tell us about Congress's views toward encryption is that Congress has concerns about encryption but doesn't know what to do about them.

Even though CALEA doesn't tell us much about congressional views on encryption specifically, it does provide some general guidance about how Congress may approach the issue.

The first lesson from CALEA is that Congress is willing to impose affirmative assistance obligations on firms. A central question underlying CALEA was whether Congress would require telecommunications

235. For instance, such legislation, championed by the FBI, was proposed in 1997, 2010, 2013, and again in 2016. *See supra* note 193. For an example of past legislative efforts, see The Electronic Data Security Act of 1997, 105th Cong. (1st Sess. 1997), https://epic.org/crypto/legislation/edsa_397draft.html [https://perma.cc/6HLA-GZTQ]; *see also* Ellen Nakashima, *Proposal Seeks to Fine Tech Companies for Noncompliance with Wiretap Orders*, WASH. POST (Apr. 28, 2013), https://www.washingtonpost.com/world/national-security/proposal-seeks-to-fine-tech-companies-for-noncompliance-with-wiretap-orders/2013/04/28/29e7d9d8-a83c-11e2-b029-8fb7e977ef71_story.html [https://perma.cc/ULB5-WJUN]; Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES (Sept. 27, 2010), http://www.nytimes.com/2010/09/27/us/27wiretap.html [https://perma.cc/X6CN-EQPP]. The most recent effort was the Compliance with Court Orders Act of 2016, proposed by Senators Burr and Feinstein. *See* Press Release, Office of Senator Dianne Feinstein, Intelligence Committee Leaders Release Discussion Draft of Encryption Bill (Apr. 13, 2016), https://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649 [https://perma.cc/HST6-ZV7Q].

236. For instance, the Security and Freedom through Encryption (SAFE) Act, introduced in 1996, would have "affirm[ed] the rights of United States persons to use and sell encryption and to relax export controls on encryption." H.R. 3011, 104th Cong. (1996). This past year, legislation was introduced in the House that would prohibit individual states from restricting the use of encryption. *See* ENCRYPT Act, H.R. 5428, 114th Cong. (2016), https://lieu.house.gov/sites/lieu.house.gov/files/documents/LIEU_027_xml%20%28ENCRYPT%20Act%20of%202016%29.pdf [https://perma.cc/WU92-FHTW].

carriers to design their networks to support law enforcement requirements. As discussed above, CALEA resoundingly answers this question in the affirmative.[237] This ought not be a surprise, as the law often imposes law enforcement assistance requirements on third parties.[238] The seemingly remarkable thing about CALEA is that it imposes an affirmative ex ante obligation on third parties to design their systems so as to be capable of providing such assistance in the future. While this is certainly a normatively contentious obligation, it is also not a surprising one. Legislatures frequently impose design obligations in order to stave off foreseeable future problems. Building codes imposing ingress and egress design requirements, for instance, aren't just about ensuring safe construction practices: they are about preventing irremediable future problems.[239] Similarly, the design of the banking system is regulated to ensure banks retain sufficient capital to cover anticipated withdrawals.[240] And the Americans with Disabilities Act imposes prospective design requirements on businesses to ensure that disabled individuals are able to participate in the world as fully as possible.[241] In each of these cases the law imposes affirmative design obligations on some parties in order to protect important social values. CALEA's obligations are no more than an application of this principle.

A second, related, lesson is that Congress may impose ex post assistance obligations upon firms. Indeed, the House Report makes clear that under CALEA, ECPA's assistance requirements continue to apply to telecommunications carriers.[242] ECPA's assistance requirement is illustrative of the potential scope of these requirements. Under it, law enforcement can receive an order directing that third parties "shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception."[243] The only limitation on this authority is that third parties "furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses."[244]

---

237. *See supra* notes 114–116.

238. *See* Morrison, *supra* note 209 (discussing the All Writs Act); *see also* 18 U.S.C. § 2518(4) (2012).

239. *See, e.g.*, Massachusetts Building Code, 780 CMR 914.0 (2008).

240. *See generally* Eric Posner, *How Do Bank Regulators Determine Capital-Adequacy Requirements?*, 82 U. CHI. L. REV. 1853 (2015).

241. Americans with Disabilities Act, 42 U.S.C. § 12101(a)(7)–(8) (1990) ("Congress finds that . . . the Nation's proper goals regarding individuals with disabilities are to assure equality of opportunity, full participation, independent living, and economic self-sufficiency for such individuals; and the continuing existence of unfair and unnecessary discrimination and prejudice denies people with disabilities the opportunity to compete on an equal basis . . . .").

242. H.R. REP. NO. 103-827, at 22 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3504.

243. 18 U.S.C. § 2518(4) (2012).

244. *Id.*

Turning to the structure of CALEA, we find more lessons about how Congress may approach the regulation of encryption. CALEA's capabilities requirements are carefully structured. Instead of imposing them on all participants in the telecommunications marketplace, or at every point in the telecommunications network, it focuses its attention on the hubs in the network — the choke points through which most traffic flows.[245] Importantly, the location of these hubs is changing. At the time CALEA was adopted, most relevant traffic would flow through a monopoly local exchange carrier. This is no longer the case: on the one hand, there are many carriers offering access to telecommunications networks today, and, on the other hand, there may be other points in modern networks that are better hubs on which to impose obligations. For instance, almost all modern cell phones run one of two operating systems (Android or Apple iOS), but they can connect to telecommunications networks via a number of network access points (including by roaming on almost any modern cellular network or via any Wi-Fi access point). In a network with this architecture, if we are to implement interception capabilities, it makes more sense for them to be incorporated into the design of these two operating systems rather than implemented on each of the tens or even hundreds of network access points that a given phone may have opportunity to communicate with in a given day. Another lesson related to the idea of imposing obligations on hubs is that assistance obligations should focus on the boundaries between modules in the network — the points of ingress and egress into each network.[246]

CALEA also continues the long tradition of recognizing a difference between content ("communications," in the language of CALEA) and metadata ("call-identifying information" in CALEA).[247] This is one of the most fundamental distinctions in Fourth Amendment jurisprudence, so it is unsurprising to see it maintained here. Perhaps unintentionally, CALEA draws this distinction in the context of encryption: the encryption exemption applies only to communications, excluding call-identifying information. As a technical matter this may be a moot distinction; traditional telecommunications carriers need unencrypted access to most of this information in order to complete calls, so it would never be the case that (most of) this information actually could be encrypted. At the same time, it is surely possible to design a communications network that allows for much of this information to be encrypted — indeed, that is one of the purposes of the Tor project.[248]

---

245. *See supra* note 175 and accompanying text.

246. *Id.*

247. *See supra* notes 46–51, 113 and accompanying text.

248. *See What is Tor?,* TOR, https://www.torproject.org/docs/faq.html [https://perma.cc/D6JH-KABV] ("[I]t prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.").

A final lesson doesn't come from the statute itself, but is seen in the discussion of it above: as a descriptive matter, any efforts to ensure law enforcement access to encrypted information will be ineffective against some subset of determined, reasonably sophisticated, adversaries. In particular, terrorists and criminals who wish to maintain the confidentiality of their communications will always have access to tools that allow them to do so. The algorithms underlying basic encryption protocols are well understood, effective, and accessible to those who need to establish a basic cryptosystem. And, relatedly, as a normative matter it is desirable that some level of encryption be readily available in order to protect important economic, social, and political institutions. This is particularly true of political dissidents in repressive regimes. The rules that we impose on encryption within the United States can affect the availability of and access to effective encryption technologies elsewhere in the world, and we need to be cognizant of those potential effects.

VI. POSSIBLE LEGISLATIVE APPROACHES TO ENCRYPTION

Despite pressure from both sides, Congress has not taken a strong position to date on the legality of encryption.[249] The introduction of strong, mass-market, end-to-end encryption will likely change this. Until recently, encryption was primarily used in commercial and infrastructure settings[250] — applications where law enforcement generally need not worry about cooperation with lawfully executed warrants. Outside of this context, encryption was primarily used by individuals with particular concerns or motivations animating their use of encryption, such as criminals or individuals concerned about political reprisal, and privacy and security researchers and advocates. It was not particularly easy to obtain or use encryption software, so those using such software had to be willing to invest a modest level of time and resources in the effort. Even had Congress outlawed the use or distribution of encryption software entirely, these individuals had demonstrated sufficient interest and acumen such that they would likely still be able to obtain and use such software.

This is different in a world in which the primary communications devices used by tens, or even hundreds, of millions of Americans incorporate easy-to-use encryption. And encryption is on a trajectory to

249. As seen above, in the years since CALEA, in which Congress expressly declined to take a strong stance regarding the legality of encryption, legislation that would both increase and decrease restrictions on encryption has been proposed. The exception to the assertion that Congress has not taken a strong stance regarding the legality of encryption is in the context of export controls. *See generally* Mark Pasko, *Re-Defining National Security in the Technology Age: The Encryption Export Debate*, 26 J. LEGIS. 337 (2000).

250. *See supra* notes 64–66 and accompanying text.

become more widespread, incorporated deeper into more consumer-grade devices, as time goes on. Before now, Congress was free not to act because the users of encryption to be targeted by congressional action either would not likely be affected by that action or used encryption in what could be considered socially valuable contexts that would possibly be harmed by such action. This has changed as encryption has become more widely deployed and easier to use.

This Part considers possible directions that Congress may take in addressing encryption. It starts by discussing the polar extremes — effectively banning encryption and fully deregulating it — as ideas that Congress is unlikely to pursue. This Part then considers more viable approaches: requirements to retain certain metadata in unencrypted form, tailoring requirements to focus only on mass-market scale platforms and services, and imposing prospective decryption assistance standards on those designing cryptosystems.

In thinking about what such legislation may look like, we should also consider its scope. Unlike CALEA, which focuses narrowly on communications traversing telecommunications carriers' networks, the modern technological setting is one in which the lines between telecommunications, information services, remote storage, and local storage are blurry and fading. Encryption is no longer about wiretapping or ECPA, or otherwise about accessing information in the context of a specific information domain. Legislation that attempts to address the use of encryption from one domain will only invite arbitrage between domains, leading to inevitable litigation and implementation delays. Rather, congressional action on encryption should address encryption directly, imposing requirements that will apply generally, across domains.

A. What Do We Not Do?

The two most frequently advocated, but also least tenable, legislative approaches to encryption are to either ban, or otherwise substantially weaken, the use of encryption or, alternatively, to fully liberalize its use. Both approaches are ill-advised, but both merit discussion.

1. Ban, or Otherwise Substantially Weaken, Encryption

The most controversial proposed legislative and policy approaches to encryption are those that would ban its use, require third parties to be able to decrypt any encrypted information, or require third parties to use encryption that the government can decrypt on its own (either

through escrowed keys or other backdoors in the encryption algorithm).[251] Such approaches are ill-advised for a number of reasons.

First, outright bans are largely ineffective and have substantial collateral consequences. To the extent that sophisticated targets — such as those generally of interest to the national security and intelligence communities — view encryption as a valuable tool they will by and large not be affected by bans, because the mathematics underlying encryption are widely understood and software implementations are widely available (and would likely continue to be, even if made illegal). And, on the other side of the ledger, encryption serves many important purposes, so the cost of a ban would be great. Encryption is essential to the modern digital economy, for instance. Outright bans on the technology would come at substantial costs.

Unsurprisingly, therefore, most legislative and policy proposals relating to encryption seek to weaken it in order to ensure that lawful government actors are able to obtain decrypted copies of information while preserving encryption's general functionality. This generally takes one of two forms: either key escrow systems, where the government has its own key that can be used to decrypt encrypted information, or algorithmic weakening, where weaknesses are introduced into the underlying encryption algorithm that enable the government to decrypt encrypted information even without its own key.[252]

---

251. As discussed above, such laws have been considered in the United States on a number of occasions. *See supra* notes 224, 235. In recent years, a number of countries around the world have considered or enacted similar legislation, including Brazil, Canada, Chile, China, France, Russia, and the United Kingdom. *See*, *e.g.*, Kevin Collier, *The Countries That Are Considering Banning Encryption*, VOCATIV (Apr. 11, 2016), http://www.vocativ.com/307667/encryption-law-europe-asia [https://perma.cc/PGG8-X8TQ]; Chine Labbe et al., *France, Germany Press for EU Encryption Law After Attacks*, REUTERS (Aug. 23, 2016), http://www.reuters.com/article/europe-attacks-france-germany-idUSL8N1B41UM [https://perma.cc/T3LP-YB4L]; Daniel Leblanc, *Privacy Watchdogs Warn Ottawa Not to Expand Surveillance Powers*, THE GLOBE & MAIL (Dec. 6, 2016), http://www.theglobeandmail.com/news/politics/privacy-watchdogs-warn-ottawa-not-to-expand-surveillance-powers/article33213678 (last visited May 5, 2017); Alec Luhn, *Russia Passes 'Big Brother' Anti-Terror Laws*, THE GUARDIAN (June 26, 2016), https://www.theguardian.com/world/2016/jun/26/russia-passes-big-brother-anti-terror-laws [https://perma.cc/95V3-3ZSW]; Gedalyah Reback, *5 EU States Demand Better Police Freedoms to Break Encryption As UK Implements Surveillance Law*, GEEKTIME (2016), http://www.geektime.com/2016/11/26/5-eu-states-demand-better-police-freedoms-to-break-encryption-as-uk-implements-surveillance-law [https://perma.cc/CK57-EPQD]. Most recently, following the Apple iPhone case, Senators Burr and Feinstein proposed draft legislation, the Compliance with Court Orders Act of 2016, which would have required entities covered by the law to be able to provide the government with any information or data transmitted using their services in "intelligible" (that is, unencrypted) form. *See supra* note 235.

252. The U.S. Government has considered both approaches, in various forms. EES, discussed above, is an example of an escrow model. And there have long been concerns that the government has worked to introduce bespoke weaknesses into encryption algorithms that it knew how to exploit. *See, e.g.,* Russel Brandom, *How Far Did the NSA Go to Weaken Cryptography Standards?*, THE VERGE (Sept. 11, 2013), http://www.theverge.com/2013/9/11/4718694/how-far-did-the-nsa-go-to-weaken-cryptography-standards [https://perma.cc/

Unfortunately, weakening encryption is often tantamount to banning it. The basic problem with efforts to weaken encryption is that it is almost impossible to implement weakened encryption in a way that doesn't effectively render it useless.[253] Most people who learn about systems like key escrow, where the government or some third party has a second key to decrypt encrypted information, believe that the second key itself is the problem with the system: Surely hackers or other nefarious parties are going to obtain a copy of that key, at which point the encryption has been compromised. While this is a significant risk, it is not the greatest problem. The real problem is that it is simply very, very difficult to design a secure multi-party cryptosystem, and it is even more difficult to correctly implement that design.[254] This was famously seen in the example of EES and the Clipper Chip.[255] The problem is that it is remarkably difficult to correctly implement even simple encryption systems — a fact that can be seen in the long history of security vulnerabilities found in encryption-related software and systems.[256] And this difficulty grows exponentially with the complexity of the algorithm. Multi-party cryptosystems are more complicated than two-party systems, which means that they are much more likely to have faults that render them ineffective.

F43U-E7TU]; Joseph Menn, *Exclusive: Secret Contract Tied NSA and Security Industry Pioneer*, REUTERS (Dec. 20, 2013), http://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220 [https://perma.cc/PN2T-TRKJ].

253. See Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, 1 J. CYBERSECURITY 69 (2015).

254. *See supra* notes 233–234 and accompanying text.

255. *Id.*

256. There have been almost too many examples of cryptosystem implementation problems in recent years to count. Perhaps the best known is the Heartbleed bug, which affected a common implementation of core cryptographic functions used widely across the web. *See The Heartbleed Bug*, HEARTBLEED.COM (Apr. 29, 2014), http://heartbleed.com [https://perma.cc/ZGG4-8UC6]. Shortly after that vulnerability was discovered, flaws in the Apache web server's implementation of the Diffie-Hellman algorithm were found (Apache is one of the most commonly used web servers on the Internet). *See Weak Diffie-Hellman and the Logjam Attack*, WEAKDH.ORG (May 20, 2015), https://weakdh.org [https://perma.cc/5ASG-ZXQ9]. There have been a number of security incidents relating to Certificate Authorities — institutions that provide and manage the cryptographic certificates used in public key infrastructure. *See* Dennis Fisher, *Final Report on DigiNotar Hack Shows Total Compromise of CA Servers*, THREATPOST (Oct. 31, 2012, 2:49 PM), https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170 [https://perma.cc/X5LN-54P8]; Woody Leonard, *Weaknesses in SSL Certification Exposed by Comodo Security Breach*, INFOWORLD (Mar. 24, 2011), http://www.infoworld.com/article/2623829/authentication/weaknesss-in-ssl-certification-exposed-by-comodo-security-breach.html [https://perma.cc/CML3-KPNV]. Indeed, the very first encryption system implemented in a web browser, SSL 1.0 implemented in Netscape Communicator in 1993, was compromised before it was even shipped to the public; a new system, SSL 2.0, was developed prior to the public release. *See* ROLF OPPLIGER, SSL AND TLS: THEORY AND PRACTICE 68–69 (2009); *see also* Phillip Hallam-Baker, *[Cryptography] Crypto Standards v.s. Engineering Habits — Was: NIST About to Weaken SHA3?*, METZGER, DOWDESWELL & CO. (Oct. 3, 2013, 5:17 AM), http://www.metzdowd.com/pipermail/cryptography/2013-October/018041.html [https://perma.cc/P57Q-NBEF].

2. Fully Liberalize Encryption

Encryption advocates have long argued that the government cannot and should not regulate the use of encryption — and this has long been the de facto policy of the United States. Despite a number of (unsuccessful) efforts to enact statutes that would place limits on the domestic use of encryption, the government has never restricted it.[257] And, despite the government's regulation of the export of encryption out of the United States for many years, today that too is effectively unregulated.[258]

At the same time, the availability and use of encryption has not historically been an immediate concern. Encryption has been an important topic for national security, law enforcement, and parts of the technology and civil liberty communities since the Crypto Wars began. But concerns about encryption have largely been hypothetical or prospective, focusing on the potential for widespread use of encryption and the issues that such use could create. As long as use of encryption has not been widespread, the prospect of restricting its use has been unappealing.[259]

After many years of hypothetical and prospective concerns, encryption's tide is turning. For various political, technical, and economic reasons, over the past few years a number of firms have begun incorporating very powerful encryption features into mass-market consumer-grade products and services.[260] The highest profile example of

---

257. *See supra* note 235 and accompanying text. The most recent such effort along these lines followed the Apple iPhone case. In response to state-level proposed legislation that would have limited firms' ability to sell products incorporating strong end-to-end encryption within a given state, Representative Ted Lieu introduced a bill that would have preempted any state efforts to limit to the use of encryption technology. *See* H.R. 4528, 114th Cong. (2016); *see also Congressmembers Lieu, Farenthold, Delbene, and Bishop Introduce ENCRYPT Act*, U.S. REPRESENTATIVE TED LIEU (Feb. 10, 2016), https://lieu.house.gov/media-center/press-releases/congressmembers-lieu-farenthold-delbene-and-bishop-introduce-encrypt-act [https://perma.cc/P35N-LVFP].

258. *See supra* note 249.

259. To be somewhat more precise, encryption *has* been widely deployed and used to secure communications while in transit and, to a lesser extent, to secure information that is in storage. For instance, web servers and browsers have supported encrypted communications since the mid-1990s, which has been essential to the advent and rise of e-commerce. Encryption has not, however, been widely used by individual end-users in a way that only they have the ability to easily decrypt the encrypted information — and especially not in the communications context. For instance, HTTPS, the protocol that allows for encrypted communications between web browsers and web servers, only encrypts communications between a user and, for example, his or her bank, e-mail provider, or social network. Once that information reaches the web server, it is decrypted such that the receiving party (e.g., Citibank, Gmail, or Facebook) has access to the transmitted information in unencrypted form.

260. The greatest pressure for this turn to implementation of widespread encryption resulted from Edward Snowden's disclosure of the extent to which technology firms had cooperated with the NSA. Apple — the biggest corporate proponent of encryption today — was particularly embarrassed by the Snowden disclosures. *See* Rob Price, *Tim Cook Defended Apple's Approach to Security: 'Encryption is Inherently Great'*, BUSINESS INSIDER (Oct. 3,

this is surely recent versions of Apple's iPhone.[261] But other services and products have followed along, including some Android-based cellular phone manufacturers and high-profile messaging services like Facebook and WhatsApp. This widespread availability and use of encryption fundamentally alters the calculus and makes it much more important that Congress act, and more likely that it will.

The political tide is also turning in favor of some level of regulation both in the United States and around the world.[262] This is most poignantly a result of the ongoing tragic wave of terrorist activities. There is evidence that terrorists have used mass-market encryption both in planning and carrying out many of these attacks and, probably more problematic, in the day-to-day operation and maintenance of their organizations.[263] But while the use of encryption by terrorists provides an acute argument for regulation of encryption, an even more forceful argument for regulation of encryption will likely come from the use of encryption in common criminal activity. The power of encryption to keep material out of the hands of law enforcement is increasingly common knowledge within criminal communities,[264] and the inaccessibility of information is a growing problem for police departments.[265]

Given these shifts, proponents of encryption should expect to see encryption regulation, and should be willing to participate in defining its contours. On the technical side, it is easier to build capabilities requirements into products at the design stage than to retrofit those products later. This is particularly true with encryption systems, which can be designed in ways that make most government assistance capabilities effectively impossible. Those approaching encryption from a civil liberties perspective also have reason to embrace a regulatory effort, as doing so now before there is a more exigent demand for regulation may

---

2016, 7:05 AM), http://www.businessinsider.com/watch-video-apple-ceo-tim-cook-encryption-security-steve-jobs-life-lessons-business-2016-10 (last visited May 5, 2017); *see also NSA Prism Program Slides*, THE GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document [https://perma.cc/XA2E-2XGQ]. The modern importance of e-commerce and the large number of data breaches in recent years have created substantial consumer interest in and demand for encryption technologies. And, after multiple decades of development and refinement — along with increased computational power of modern devices — it is technologically easier than ever to implement encryption.

261. *See supra* Section V.A.

262. *See supra* note 251.

263. *See supra* note 205.

264. *See* Mark Berman, *Police Say Criminals View iPhone as 'Another Gift from God' Because of the Encryption*, WASH. POST (Mar. 18, 2016), https://www.washingtonpost.com/news/post-nation/wp/2016/03/18/police-backing-the-fbi-in-fight-with-apple-say-criminals-love-iphones-and-call-the-encryption-a-gift-from-god [https://perma.cc/T7RC-RZHY].

265. *See*, *e.g.*, MANHATTAN DISTRICT ATTORNEY'S OFFICE, Report on Smartphone Encryption and Public Safety (2016); Cat Zakrzewski, *Encrypted Smartphones Challenge Investigators*, WALL ST. J. (Oct. 12, 2015, 7:36 PM), http://www.wsj.com/articles/encrypted-smartphones-challenge-investigators-1444692995 [https://perma.cc/F2GP-SXMH].

present the best opportunity to advocate for the least onerous restrictions possible.[266] This is particularly important in the civil rights context due to the very concerning approaches to encryption being advanced in other countries.[267] If the United States engages in a serious discussion about possible approaches to regulating encryption today, the discussions we have will have some ability to set standards and moderate approaches set elsewhere — including in countries with less regard for civil rights. If, however, advocates in the United States maintain a stalwart opposition to any regulation of encryption, they may lose a valuable opportunity to moderate discussions occurring both in the United States and abroad.

B. What Might We Do?

There is a wide range between the two poles rejected above, in which we can find a number of possible forms of regulation that we could impose upon encryption. These approaches are drawn from the features and structure of CALEA previously discussed. They are presented at a general level. Each could be implemented in any number of ways; the purpose here is to put ideas on the table for further discussion and development through the political process, not to spin out detailed legislative proposals. And they are not mutually exclusive — each could be implemented in combination with the others.

1. Impose Retention Obligations for Certain Metadata

A first possible approach follows the traditional distinction between content and metadata that has been developed by the Supreme Court and incorporated into ECPA and similar statutes.[268] Under this

266. Gus Hurwitz, *The US Gave Up on Being a Leader on Encryption. China and Russia Are Eager to Step in.*, TECHPOLICYDAILY.COM (Dec. 8, 2016, 6:00 AM), http://www.techpolicydaily.com/technology/us-gave-leader-encryption-china-russia-eager-step/ [https://perma.cc/8B35-FENA].

267. For examples of other countries that are considering or have adopted restrictions, see *supra* note 251. Russia, for instance, has enacted legislation that requires encryption backdoors. *See* Mike Masnick, *Putin Says All Encryption Must Be Backdoored in Two Weeks*, TECHDIRT (July 8, 2016, 10:42 AM), https://www.techdirt.com/articles/20160708/07535134919/putin-says-all-encryption-must-be-backdoored-two-weeks.shtml [https://perma.cc/98AP-LTLF]. China has enacted legislation that requires firms to provide "technical support" to government investigations, which may include decryption assistance obligations. *See* Bruce Einhorn, *A Cybersecurity Law in China Squeezes Foreign Tech Companies*, BLOOMBERG (Jan. 21, 2016, 4:14 PM), https://www.bloomberg.com/news/articles/2016-01-21/a-cybersecurity-law-in-china-squeezes-foreign-tech-companies [https://perma.cc/43MZ-6T93] ("[T]he law's vague wording on when and how to help law enforcement decrypt data 'leaves concern about how companies will be expected to carry this out.'"); *see also Final Passage of China's Cybersecurity Law*, BAKER MCKENZIE (Nov. 25, 2016), http://www.bakermckenzie.com/en/insight/publications/2016/11/final-passage-of-chinas-cybersecurity-law/ (last visited May 5, 2017).

268. *See supra* notes 46–51, 113 and accompanying text.

approach, products, services, and devices would be free to make use of strong encryption, subject to the requirement that some information (identified here as metadata) be preserved, retained, or otherwise available in unencrypted form. Defining what is classified as metadata is an inherently political, legal, and technical process, but one can imagine the range of information that could be classified as such. Such information could conceivably include: contact lists or recent contacts, lists of applications installed on a device and a listing of recently used applications, or a listing of files on a device or recently accessed or modified files. Alternatively, instead of classifying metadata broadly by content type, it could be classified structurally: devices and applications could be limited to using strong encryption to store user data, ensuring the data and settings of applications remain available to law enforcement.

At a technical level, such requirements could be implemented in a number of ways. Ideally any legislation would follow the model used in CALEA and specify only the capability requirement, leaving implementation to individual developers or industry standard setting processes. For the sake of demonstrating a minimum level of viability, one could imagine implementing such a capability requirement by segregating different types of data on separate partitions, each encrypted with a separate key: one user-defined and not recoverable, and another either defined by the developer or recoverable from the device, product, or service itself. Indeed, recent versions of Apple's iOS operating system implement a multiple-key system somewhat similar to this; the principal technical difference is that each of those keys is itself encrypted using the user's own key.[269] An alternative approach would be to include multiple copies of metadata information on the device, one comingled with content information and encrypted with an unrecoverable key, and one separate and recoverable by law enforcement.

Critically, neither of these approaches requires developing any new encryption technologies — or compromising existing ones. Indeed, they only require implementing existing technologies in ways that they have already successfully been used in the past.

269. *See generally* APPLE, *iOS Security* (2016), https://www.apple.com/business/docs/iOS_Security_Guide.pdf [https://perma.cc/FU23-5TGA]. More precisely, most of the device's encryption keys are a function of both the user's passcode key (defined by the user's PIN or password) and a separate, device-specific key that is inaccessible to both the user and Apple (the hardware or device UID key). Different types of information are encoded using different keys ("class keys") depending upon how that information is classified. Each of these class keys is created by combining the passcode key, the hardware key, and the classification-specific class key. *Id.*

2. Impose Capabilities Requirements on Mass-Market Products and Services

A second possible approach would impose more capabilities requirements — requirements that could substantially limit the use of encryption altogether — but impose them only upon a tailored subset of products, services, and devices that may serve as bottlenecks: perhaps those operating at a sufficiently large scale and that are available on a consumer-oriented, mass-market basis.

This is the basic functional structure used by CALEA. CALEA imposed capabilities requirements on telecommunications carriers because they were the architecturally logical and efficient place to do so, not because there is any inherent reason that such obligations ought to be imposed on telecommunications carriers. Rather, it is most efficient to intercept communications at communication hubs' ingress and egress points.[270] In the 1990s, when most network access was facilitated by a monopoly telecommunications carrier and the Internet was the Wild West, it made sense to impose capabilities requirements only upon the carrier. Today, the hubs are smartphones and a small number of apps running on them. The iPhone, Facebook, Twitter, WhatsApp, Gmail — each of these operates on a scale comparable to only the largest telecommunications carriers in the United States (and much larger than most carriers today).[271]

As a matter of historical accident, we naturally think of traditional telecommunications carriers — that is, telephone companies — as regulated monopolies and therefore accept the idea of imposing regulatory obligations upon them. And we traditionally have imposed much lower

---

270. *See* H.R. REP. NO. 103-827, at 18 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3498 ("Earlier digital telephony proposals covered all providers of electronic communications services, which meant every business and institution in the country. That broad approach was not practical. Nor was it justified to meet any law enforcement need.").

271. Verizon Wireless and AT&T are the largest traditional telecommunications carriers in the United States, with approximately 141 and 129 million users, respectively. *See* FED. COMMC'NS COMM'N, DA 16-1061, NINETEENTH REPORT 11 tbl.II.B.1 (Sept. 23, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DA-16-1061A1.pdf (last visited May 5, 2017). Most others among the large telecommunications carriers (including both traditional landline telephone and Internet services) have well under 100 million subscribers. Indeed, today there are fewer than 135 million *total* retail landline telephone customers in the United States, spread across all carriers. *See id.*; *see also* FED. COMMC'NS COMM'N, *Local Telephone Competition: Status As of December 31, 2013* (Oct. 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-329975A1.pdf (last visited May 5, 2017). In the United States alone, Facebook has over 182 million active daily users and Apple has over 94 million iPhone owners — and both have many times more worldwide. *See* Company Information Page, FACEBOOK, http://newsroom.fb.com/company-info/ (last visited May 5, 2017) (reporting 1.23 billion active daily Facebook users, of which approximately 14.8 percent are in the United States); Don Reisinger, *iPhones in Use in the US Rise to 94M, New Study Suggests*, CNET (May 15, 2015), https://www.cnet.com/news/nearly-100m-iphones-in-use-in-the-us-new-study-shows [https://perma.cc/CKA9-W3CU].

regulatory obligations, if any at all, on device manufacturers and information companies like Apple and Facebook. But this distinction is increasingly irrelevant. If anything, Facebook and the iPhone, entry points into the network, are both more efficient and likely more effective than telecommunications carriers in intercepting potentially encrypted communications. Moreover, the near complete hybridization of telecommunications carriers and information services largely renders the technological distinction moot. In this day where telecommunications services can be provisioned as information services and information services can be provided from within a telecommunications network, it is far more appropriate to take a functional approach when allocating these regulatory burdens.

As with the previous approach, specific implementation details are not developed here. For instance, it is non-trivial to define "mass-market," or the appropriate metric of scale for determining whether a service, product, or device should be subject to capabilities requirements. In this sense, CALEA had things easy since it was able to free-ride on telecommunications carriers' traditional monopoly and regulated statuses. But as technology has evolved, it has become less clear as to what type or types of entities should be targeted by the imposition of capabilities requirements. And there is also the question of how the capabilities requirements ought to be implemented and what types of information they ought to cover. Here, too, the best approach would likely follow the traditional content/metadata distinction. Indeed, as we transition to imposing capabilities requirements on information services, one could think of these requirements as an update to the Stored Communications Act, paralleling CALEA as an update to the Wiretap and Pen Register Acts. If nothing else, it may make sense to take the Stored Communications Act's bifurcation of records (metadata) and content as a starting point for considering what data needs to be available to law enforcement and on what terms.

3. Impose Prospective Decryption Assistance Requirements

A final possible approach draws upon the House Report's reminder that the Wiretap Act's existing assistance requirements continue to apply in light of CALEA.[272] Congress could more expressly define what assistance needs to be provided to law enforcement that encounters encrypted communications.

This idea is particularly important in light of Apple's approach to end-to-end encryption. The discussion of encryption, and of the assistance requirement, in CALEA and the House Report was written with

272. H.R. REP. NO. 103-827, at 22, *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3504 (discussing the responsibility of a telecommunication carrier in a manner "consistent with the obligation to furnish all necessary assistance under 18 U.S.C. Section 2518(4).").

AT&T's TSD-3600 secure telephone in mind. When using this phone, the process of encryption, including the negotiation and distribution of encryption keys, was entirely out of the telecommunication carrier's hands. AT&T provided the encryption product, but it was a product that produced output that AT&T was unable to decrypt, so CALEA's encryption exemption applied.

But this does not mean that AT&T would not have been under any obligation to law enforcement with respect to these communications. The assistance provision requires any requested third party to provide, among other things, all information and technical assistance to accomplish an interception.[273] While no such case was ever litigated, it is very possible that AT&T could have been compelled, even against its own potential objections, to provide law enforcement with detailed technical information about the operation of the TSD-3600 — likely including complete schematics, documentation, and source code and other programming information for the device.

It is less clear how the assistance requirement would be applied in the contemporary setting, such as to iPhones and similar devices. There are at least two foreseeable challenges to the use of the assistance provision in this case. The first is that Apple would likely strenuously object to releasing its source code to the government. And, for that matter, the government likely would not be able to meaningfully use that source code without significant assistance and documentation from Apple. The second difficulty is, frankly, fascinating. Apple has designed its modern iPhones to have a secret unique device ID (so secret, in fact, that not even Apple knows or can determine what it is) contained on a physical chip in the phone.[274] This device ID is used as part of the device's encryption key — you need it in order to decrypt the contents of the phone.[275] But Apple designed the iPhone such that the device ID is inaccessible to anyone. The iPhone's internal circuitry can use the device ID when calculating encryption keys — but there is no way for it to share the device ID itself.[276]

In other words, Apple has designed its recent iPhones in a way that makes it technologically impossible for anyone — Apple or the user of any iPhone — to provide all of the information necessary to decrypt the information on the device. Rather, any efforts to decrypt the information on a given iPhone have to be undertaken using the iPhone itself.

It is unclear how a court would respond to this. The technology that Apple has developed was not in Congress's mind when it drafted CALEA. To the contrary, Congress had a very specific, and very different, technology in mind. The TSD-3600 used strong encryption, but

273. *See id.*; *see also* 18 U.S.C. § 2518(4) (2012).
274. *See supra* note 269.
275. *Id.*
276. *Id.*

it left a trail of metadata as it traversed the network that was still available to law enforcement, and it was generally (if not always) tied to a specific phone and phone line, such that law enforcement could rely upon other non-wiretap tools to obtain the contents of calls. Apple's technology doesn't merely encrypt the communications channel: it is meant to prevent as much information leakage as possible, and it is meant to ensure that Apple itself cannot decrypt its users' communications. One could easily see a judge finding that Apple, having designed a technology that leaves it with no assistance to give law enforcement, is in compliance with ECPA's assistance obligations; but one could just as easily see a judge sanctioning Apple for non-compliance on the grounds that Apple designed its products in order to make compliance impossible.

Rather than rely on the vicissitudes and happenstance of whatever judge happens to first confront this issue, Congress would be well advised to spell out in greater detail the assistance obligations that firms face when dealing with law enforcement efforts to obtain encrypted information. For instance, one could imagine (and I would recommend) requiring firms to provide law enforcement with either actual or reference implementations of any encryption algorithms, along with technical documentation about the details of the algorithm. And one could imagine (and again I would recommend) that firms be required to provide law enforcement with all information necessary to decrypt encrypted information except for keys that are either under the sole custody of the user (for example, PINs and passwords) or that are dynamically generated on a per-use basis (such as with the Diffie-Hellman key exchange algorithm). And, as a final recommendation, one could imagine requiring that firms be able to extract a bit-perfect copy of all encrypted information stored on a device, such that law enforcement can undertake its own efforts, on its own equipment and with its own personnel and resources, to break the encryption. Absent these requirements, law enforcement is effectively beholden to the past and present design decisions of manufacturers and service operators, which are currently made without any affirmative obligations to support data requests. This could be construed as an inappropriate usurpation of and interference with the legal authority vested in law enforcement.

These specific recommendations unquestionably contain embedded policy preferences, and so should be the subject of discussion and debate. One of the most important of these preferences bears highlighting: whether the level of protection afforded to a user's information should be concomitant to that user's own effort to protect her information. If a user takes specific measures to avail herself of greater protection — for instance, by enabling non-standard settings that allow more complex passwords or PINs than a device enables by default —

that provides important information about her subjective privacy expectations. If, on the other hand, a user chooses to use a poor password or a short PIN, that may suggest a lesser expectation of privacy. Such inferences are made more difficult when a firm chooses defaults that tend to indicate high expectations of privacy. Congress and the courts should be careful when evaluating users' privacy expectations in settings where firms are making default choices. For instance, the traditional Fourth Amendment inquiry — which is at least informative if not dispositive to questions about government access to encrypted communications — asks whether an individual has both an objective and subjective expectation of privacy.[277] But where firms are setting defaults on behalf of their users, these defaults encode the *firms'* subjective views on privacy, which are simultaneously (1) irrelevant to how we traditionally think about compelled government access to communications under the Fourth Amendment and (2) the defining characteristic over whether such access is possible (regardless of the individual users' own expectations) in the age of encryption.

VII. CONCLUSION

It is difficult to find the correct balance between the right of individuals to be secure against government intrusion and the need of the government to sometimes encroach upon that right. It pits two polar views of the purpose of government — and of American government in particular — against each other. The political history of encryption is the history of trying to maintain this balance in the face of changing technology.

Today we are in the midst of the latest iteration of technological change disrupting this balance. The advent of pervasive mobile communications platforms — smartphones — and the substantial integration of these devices with the applications that run on them has dramatically shifted the balance in favor of the individual's right to keep her information secure from the government. This is most true in the case of mass-market communications devices that enable strong end-to-end encryption by default.

This Article has used CALEA, a statute enacted both during and as a result of the last major shift in encryption technology, as a lens to consider how Congress may approach this issue in the future. CALEA itself had nothing to say about encryption — as a result of a political compromise it focused only on the access that telecommunications carriers had to give law enforcement to communications, leaving questions

277. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); Smith v. Maryland, 442 U.S. 735, 740 (1979).

about law enforcement's ability to make use of (decrypt) those communications to the future. Regardless, the history and structure of CALEA provide useful insights into congressional understanding of the encryption issue. In particular, in structuring CALEA, Congress demonstrated a relatively nuanced attention to the contemporary architecture of communications networks, placing interception capability obligations at efficient locations in the network (the communications bottlenecks through which all communications and routing information necessarily passed).

In the twenty-five years since CALEA was first proposed, two clear sides have developed in debates about encryption and their positions ossified. Proponents of strong encryption argue that the government cannot and should not regulate encryption. Law enforcement and national security interests have argued that engineers need to develop an approach to encryption that facilitates lawful government decryption. The two sides have gone back and forth for twenty-five years, with little progress being made in the interim.

This Article is an effort to make progress. It rejects both of these polar views as untenable. Rather, it uses lessons from CALEA to identify areas where common ground is possible and what that ground may look like. It argues, for instance, that certain forms of metadata can be identified and kept in non-encrypted form, while allowing other information to be secured with strong end-to-end encryption. The technology to do this exists today. This Article further argues that mass-market communications platforms — the new bottlenecks in the network, where interception capabilities could be most efficiently located — should face a higher obligation to be able to make encrypted communications available to law enforcement in unencrypted form — and that as a practical matter this will not materially affect the circumstances of those most likely to use strong encryption while significantly benefitting the legitimate needs of law enforcement. And it argues that Congress should clarify the ambiguous assistance obligations already imposed in federal law, so that law enforcement, the courts, and firms developing communications platforms understand what these obligations require. It further outlines possible clarifications that would allow firms to deploy strong encryption while ensuring that law enforcement is in the best position possible to operate in an encrypted world.

More importantly, this Article expresses the hope that common ground exists between both sides and attempts to map out some of its contours. Over the next several years, Congress will be considering — and likely adopting — legislation to address questions about encryption. Congress needs to understand that compromise is possible; and both sides to this debate, distrustful and ossified as they may be, should work to find a mutually agreeable solution based upon the common ground they likely share.