DANCING IN THE DARK: HOW END-TO-END ENCRYPTION HAS ALLOWED SOCIAL MEDIA PLATFORMS TO SIDESTEP THE LAW

NIKHIL RAO

ABSTRACT

The widespread use of encrypted messaging by social media platforms is a source of contentious public debate. Governments and law enforcement agencies argue for the need to review electronic messages to investigate and prosecute serious criminal offenses. Privacy and civil rights advocates—and the social media platforms themselves—counter that enabling greater law enforcement access will also make it easier for criminal actors to access and manipulate the private information of these platforms' users. The strongest and fastest-growing kind of encryption is called end-to-end encryption. Only the sender and intended recipient of an end-to-end encrypted message can read its contents. That is why the effect of this kind of encryption is often called "going dark"; if deleted, the message's contents are rendered completely inaccessible to any third parties. This includes the provider of the communication service, and law enforcement agencies. This Article approaches the legal issues surrounding end-to-end encryption in a different way. It will not wade into the normative, oft-discussed privacy debate. Rather, it will seek to positively explain how end-to-end encryption, as currently practiced, is not in compliance with service providers' federal statutory obligations to disclose information to law enforcement.

Table of Contents

I. Introduction

On August 24, 2024, French police arrested Pavel Durov, the billionaire founder and CEO of the infamously laxly-moderated social media platform Telegram. The dramatic arrest came as Durov disembarked from his private jet in Paris.[1] Three days later, the Paris criminal court announced the charges against him, centering on Durov's failure to prevent criminal activity on Telegram; his refusal to cooperate with law enforcement investigations of crimes committed on the platform was well known. At the time of writing, this sentiment is stated explicitly in Telegram's "Frequently Asked Questions" page: "[t]o this day, we have disclosed 0 bytes of user messages to third parties, including governments."[2, 3]

Somewhat ironically, Telegram's use of end-to-end encryption (E2EE) is extremely limited; the feature can only be manually activated for certain direct messaging chats.[4] E2EE has been much more thoroughly

[1] Romain Dillet, *France formally charges Telegram founder, Pavel Durov, over organized crime on messaging app*, TechCrunch (Aug. 29, 2024, 3:03 AM), https://techcrunch.com/2024/08/29/france-formally-charges-telegram-founder-pavel-durov-over-organized-crime-on-app/.

[2] *Telegram FAQ*, Telegram.org https://telegram.org/faq?setln=en (last visited Jan. 26, 2025).

[3] This type of statement is called a "warrant canary", drawing upon how coal miners used canaries as a warning signal for carbon monoxide in days of old. If Telegram ever removes this statement from their FAQ page, it means that they have disclosed user messages to third parties.

[4] Matthew Green, *Is Telegram really an encrypted messaging app?* A Few Thoughts on Cryptographic Engineering (Aug. 25, 2024), https://blog.cryptographyengineering.com/2024/08/25/telegram-is-not-really-an-encrypted-messaging-app/.

implemented on other social media platforms like WhatsApp and Signal,[5] as well as Apple's iMessage[6] and, very recently, Meta's Facebook Messenger.[7] A majority of Americans use at least one of these platforms, ensuring that consumers who prioritize copious levels of privacy and security on social media have a plethora of options to choose from.[8]

Nonetheless, Durov's arrest is emblematic of Western governments' concern over the practice. France is by no means alone; former FBI Director James Comey has highlighted the difficulties strong encryption methods like E2EE pose for law enforcement,[9] as have crime agencies from the United Kingdom, Australia, and the European Union.[10] Speaking broadly, law enforcement's concern is that E2EE prevents the social media

[5] Robert Dougherty, *Exploring E2EE: Real-world Examples of End-to-End Encryption*, Kiteworks (Aug. 12, 2023), https://www.kiteworks.com/secure-file-sharing/real-world-examples-of-end-to-end-encryption/.

[6] *Messages & Privacy*, Apple.com (last visited Jan. 26, 2025), https://www.apple.com/legal/privacy/data/en/messages/ .

[7] Cooper Quintin and Mona Wang, *Meta Announces End-to-End Encryption by Default in Messenger*, Electronic Frontier Foundation (Dec. 7, 2023), https://www.eff.org/deeplinks/2023/12/meta-announces-end-end-encryption-default-messenger.

[8] Stacy Jo Dixon, *Share of Facebook Messenger users in the United States as of July 2024, by age group*, Statista (Aug. 2, 2024), https://www.statista.com/statistics/951142/facebook-messenger-user-share-in-usa-age/.

[9] Dina Temple-Raston, *FBI Director Says Agents Need Access To Encrypted Data To Preserve Public Safety*, National Public Radio (Jul. 8, 2015, 7:32 PM), https://www.npr.org/sections/thetwo-way/2015/07/08/421251662/fbi-director-says-agents-need-access-to-encrypted-data-to-preserve-public-safety.

[10] Alex Hern, *Crime agencies condemn Facebook and Instagram encryption plans*, THE GUARDIAN (Apr. 20, 2023, 7:24 AM), https://www.theguardian.com/technology/2023/apr/20/crime-agencies-condemn-facebook-instagram-encryption-plans.

platform from “unlocking” the encrypted content, and therefore, being able to disclose that content to law enforcement.[11]

This article will focus on the legal ambiguities created by the technical challenge of E2EE. First, it will explain the general concepts required to understand encryption, including why and how E2EE’s challenge for law enforcement is different—and the practices by which law enforcement is currently, and inadequately, coping with this challenge. The Article will then examine that challenge in light of the rules set forth in three federal laws which most closely touch the disclosure of electronic evidence to law enforcement. These are the Stored Communications Act (SCA) of 1986, the Communications Assistance for Law Enforcement Act (CALEA) of 1994, and finally the All Writs Act (AWA) of 1789. The Article will demonstrate how E2EE’s technical characteristics make it impossible for E2EE providers to comply with the SCA, creating a disclosure problem that CALEA and the AWA ultimately fail to resolve.

[11] Temple-Raston, *supra* note 9.

II. Background: Encryption Concepts Explained

At its most basic level, encryption refers to "the conversion of plaintext to a meaningless string of gibberish (also called ciphertext) so that an eavesdropper cannot easily decipher it."[12] For example, the algorithm for a simple encrypted message might require that each letter in a string of text is shifted one place to the left in order to decrypt it. Thus, "Ifmmp, Xpsme!" becomes "Hello, World!" after we apply the shifting algorithm.[13] This kind of simple encryption arguably dates back to ancient Rome, where it was used by Julius Caesar in his military campaigns.[14] Modern algorithms are much more complicated than this simple cipher and often incorporate computerized randomization. There are two main types of encryption: symmetric and asymmetric.

The substantive difference between these two types of encryption is how they use the encryption "key." In computer science terms, the key is a string of data values that allows content to be encrypted and decrypted through complex mathematical processes.[15]

[12] Anthony G. Volini, *A Deep Dive Into Technical Encryption Concepts To Better Understand Cybersecurity & Data Privacy Legal & Policy Issues*, 28 J. INTELL. PROP. L. 291, 301 (2021).

[13] *Id.*

[14] *See* C. SUETONIUS TRANQUILLUS, LIFE OF JULIUS CAESAR 28 (Robert Graves transl., Penguin Classics 2007).

[15] *What is end-to-end encryption (E2EE)?*, Cloudfare.com (last visited Feb. 27, 2025), https://www.cloudflare.com/en-gb/learning/privacy/what-is-end-to-end-encryption/.

A lay analogy will help explain why this is so. Suppose I want to have a postman mail a letter consisting of the text “Hello, World!” to my friend. If the letter is mailed with symmetric encryption, the postman and I agree on the encryption algorithm (for example, shifting each letter one letter forward in the alphabet, and vice versa for decryption) and the verbal key, which I’ve agreed upon with my friend beforehand. Applying the algorithm to the text, the postman carries a letter saying “Ifmmp, Xpsme!” to my friend. My friend must tell the postman the same key before the postman will give him the letter and the instructions to decrypt it. The key is the same for both of us, hence the name “symmetric.” If someone tries to intercept the letter without knowing the key, they will see only that nonsense phrase “Ifmmp, Xpsme!”. But if they do know the key, the postman will assume they are my friend and they will get the full message.

Originating in academia in the 1970s,[16] asymmetric encryption is more secure than its symmetric counterpart. It avoids the liability of symmetric encryption by using two keys, a public key and a private key.[17] Each correspondent in an asymmetrically encrypted conversation will have

[16] Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, 22 IEEE TRANSACTIONS ON INFO. THEORY 644 (1976).

[17] *What types of encryption are there?*, Information Consumers Office UK (last visited Jan. 31, 2025), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/encryption/what-types-of-encryption-are-there/.

a public key, shareable with anyone, and a private key, known only to its owner. The greater security comes from the fact that an interceptor is very unlikely to know anyone's private key—whereas it would be relatively easier for them to figure out a symmetric key, as it's used at both ends of the conversation and is accordingly more vulnerable. In the letter-mailing analogy, when I give my friend's public key to the postman, my friend tells the postman his own private key to receive the letter and the decryption instructions. Only on hearing my friend's private key given in response to a message originally encrypted with my friend's public key will the postman reveal the content. Why have a public key at all, then? So you can send a message to someone without knowing their private key—which, of course, you should not know.

A. End-To-End Encryption (E2EE)

E2EE is a kind of strong encryption, usually asymmetric, that is very different to the basic kind of encryption discussed above.[18] In the *non*-E2EE methods discussed above, the platform over which an encrypted communication is sent *is* privy to that communication's content. The encrypted non-E2EE message is decrypted on the hosting social media

[18] *Supra* note 15.

platform's servers, then re-encrypted before continuing on to the recipient. But under E2EE, the message remains encrypted for the whole process without the hosting platform ever knowing the key.[19] This is why E2EE is called "end-to-end"; the encryption remains in place from one "end" of the conversation to the other "end." To be explicit, only the correspondents themselves have knowledge of the decrypted message. This is what gives rise to the descriptive phrase "going dark." Lastly, E2EE only encrypts what computer scientists call "data-in-motion", for example, messages. Data-in-motion is inherently more vulnerable to interception than "data-at-rest", such as the static data stored on a hard drive.[20] E2EE does not encrypt data-at-rest for the simple reason that if data is at rest, it does not go from one "end" of a conversation to the other.

B. The Challenge For Law Enforcement

The inherent inaccessibility of E2EE creates a unique problem for governments and law enforcement agencies. American law enforcement authorities' considerations are twofold: they want to prevent E2EE from concealing and facilitating serious criminal offenses; and they want to use

[19] *Supra* note 15.

[20] *See generally Lawful Access*, OFF. OF LEGAL POLICY U.S. DEP'T. OF JUSTICE (Nov. 18, 2022) https://www.justice.gov/olp/lawful-access.

E2EE evidence to prove the convictions of defendants accused of such offenses. Former FBI director Christopher Wray summed up the law enforcement position well when he said in a 2019 speech that "criminals… relish the ability to hide on encrypted devices and inside encrypted messaging platforms… for the common-sense reason that they think it helps them do their harm with impunity, and without detection."[21]

An unnamed criminal case from 2019 provides an instructive example of the challenge generally posed by encrypted content. Federal prosecutors in the Northern District of Ohio sought to try a suspect on child sex trafficking charges. Prosecutors knew that inculpatory evidence was contained on the suspect's encrypted cell phone because, shortly after his arrest, he revealed to an acquaintance on a jail call that "if they [law enforcement] get in my phone, I'm doing time."[22] But the government lacked the technical resources necessary to unlock the encrypted content, despite the presence of a lawfully issued search warrant. The Department of Justice's description of this case concludes by stating that "*[t]o this day*, law enforcement has been unable to access the encrypted phone and may

[21] Christopher Wray, Dir., FBI, Fordham Univ. - FBI Int'l. Conference on Cyber Security: The Way Forward Working Together to Tackle Cybercrime (Jul. 25, 2019) (transcript available at https://www.fbi.gov/news/speeches/the-way-forward-working-together-to-tackle-cybercrime)
[22] *Supra* note 20.

never get the evidence needed to prosecute the suspect for his most serious offenses" (emphasis added).[23]

This case illuminates E2EE's unique technical challenge for multiple reasons. Regardless of the cell phone's manufacturer, the encryption in this instance was almost certainly a type of very strong *symmetric* encryption of the phone's data-at-rest.[24, 25] The fact that a relatively less secure form of encryption stymied this unnamed criminal case is very important; prosecutors' failure to obtain the inculpatory evidence was due to a technical challenge *less* insurmountable than that which E2EE would have imposed. The success of the methods of overcoming such challenges are, as discussed below, "inherently probabilistic" (but by no means impossible, though they did fail here).[26] However, E2EE places technical success squarely outside the bounds of probability. Or, to put it another way, if encryption in general makes law enforcement's task difficult, then E2EE makes it practically impossible.

[23] *Id.*

[24] *Data Protection overview*, APPLE.COM (last visited Jan. 31, 2025), https://support.apple.com/en-gb/guide/security/secf6276da8a/web.

[25] *File-based encryption (FBE) and full-disk encryption (FDE)*, Samsung Knox Documentation (Feb. 20, 2024) https://docs.samsungknox.com/admin/knox-platform-for-enterprise/kbas/kba-360039577713/.

[26] Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989 (2018).

III. Current Practices For Encrypted Evidence

Law enforcement has developed various methods for overcoming the technical challenges of encrypted evidence in general. These may be divided into two categories: the relatively narrow "compelled decryption,"[27] and the relatively broad "alternative encryption workarounds."[28] Neither, as will be seen, provides a consistent technical solution to E2EE's challenge.

A. Compelled Decryption

Compelled decryption means forcing, by means of a court order, the suspect or a third party to decrypt the desired content themselves—for example, by entering a password. Such orders, of course, implicate suspects' constitutional Fifth Amendment privilege against self-incrimination.[29] The debate over whether, and to what degree, that privilege applies to such orders is outside this Article's scope.

More importantly, technical capabilities or incapabilities are simply not relevant to compelled decryption's success.[30] Rather, it is a contest of human wills—law enforcement against the suspect—and of differing

[27] Eric A. Haskell, *Gelfgatt, Jones, and the Future of Compelled Decryption*, 63-SUM Boston Bar Journal (2019).
[28] Kerr & Schneier, *supra* note 26.
[29] Haskell, *supra* note 27.
[30] Kerr & Schneier, *supra* note 26.

constitutional legal interpretations. A suspect, rational or otherwise, may certainly choose to refuse to comply with a compelled decryption court order if the total consequences of the original crime are perceived as more severe than the consequences of noncompliance.[31] So compelled decryption, even when successful in revealing E2EE content, has not actually succeeded in overcoming any technical challenge.

To avoid any Fifth Amendment interaction, might a third party with the ability to provide decryption—for example, by providing the suspect's passcode—be compelled to decrypt? First, compulsion in these instances remains primarily that contest of human wills, although levels of resistance will vary. A large social media company for whom a particular suspect is one among millions of customers may have a very different calculation than a particular suspect's "ride-or-die" friend or partner. Second, any third party is less likely than the suspect themselves to actually possess knowledge of the information required for decryption, such as a passcode.

Particularly in the case of social media platforms or other technology companies, knowledge of the key itself may be under sufficiently strong encryption as to prevent the third party from disclosing it (without the suspect's consent) *even if* the third party wanted to. That

[31] *Id.*

kind of strong encryption does not have to be restricted to asymmetric encryption, to E2EE, or even to data-in-motion, although the effect is identical. For example, Apple does not disclose any user's passcode to law enforcement (or anyone else);[32] again not because of a voluntary refusal, but because the encryption that Apple has in place to protect users' passcodes is too strong for Apple itself to reasonably overcome—*despite* the fact the encryption it uses, called AES-XTS,[33] is a kind of (very strong) symmetric encryption.[34]

In sum, methods of compelled decryption fail to provide a solution to the technical challenge imposed by E2EE, and this is true regardless of the entity being so compelled. Nor do they provide a solution to the challenge imposed by other particularly strong non-E2EE methods. Let us now turn to law enforcement's other current practices for dealing with encryption's technical challenges.

[32] *Legal Process Guidelines*, Apple.com (last visited Jan. 31, 2025), https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf.

[33] *Intro to FileVault*, Apple.com (last visited Jan. 31, 2025), https://support.apple.com/en-gb/guide/deployment/dep82064ec40/web.

[34] Morris Dworkin, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*, NIST Special Publication 800-38E (Jan. 2010), https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38e.pdf.

B. Alternative Encryption Workarounds

There are several methods in place for sidestepping encryption's protections. But because of either their technical restrictions or their dependence on case-specific circumstances, they are generally not consistently feasible or practicable. Accordingly, they do not present a workable technical solution to E2EE's challenge.

It is *theoretically* possible to break *any* encryption algorithm, but only by trying every possible combination of the values which constitute the key.[35] This is called a brute-force attack.[36] These attacks are effectively and mathematically impossible under modern encryption standards because of the immense amount of computing power required to conduct them.

That said, users seldom interface with the key in such a direct manner. More often, a phone or computer password "activates" the actual key, which then decrypts the data-at-rest; or alternatively, a communication platform's software automatically generates keys which encrypt and decrypt the E2EE data-in-motion. Of course, this process still requires that a user successfully log in to their device and then to their account on the

[35] Kerr & Schneier, *supra* note 26.

[36] *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY, SECOND EDITION: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C 151 (2d ed. 2015).

platform, with login passcodes.[37] In this sense, passcodes can be thought of as a kind of proxy key—not to be confused with the actual encryption key.

What all this means is that, in a rather limited sense, brute-force attacks are a way to overcome E2EE's unique technical challenge. Passcodes' proxy key functionality could be thought to make brute-force attacks more likely to be successful, but makers of electronic devices have instituted a variety of safeguards to counter this circumstance—such features are market manifestations of consumers' strong preference for privacy and security when their technology meets their personal information. For example, Apple infamously has an option to erase all data on its iPhones after a user-set number of incorrect passcode attempts (a number certain to be far below the 10,000 possible four-digit iPhone passcodes),[38, 39] and non-Apple devices can obtain an identical feature through third parties.[40] The upshot is that the success of a brute-force attack is entirely dependent on luck—lots of it.

[37] Kerr & Schneier, *supra* note 26.

[38] *Set a passcode on iPhone*, Apple.com (last visited Jan. 30, 2025), https://support.apple.com/en-au/guide/iphone/iph14a867ae/18.0/ios/18.0.

[39] This was the feature which temporarily thwarted the FBI in their efforts to unlock an iPhone belonging to one of the perpetrators of the 2015 San Bernardino terrorist attack. *See* Sean Hollister & Connie Guglielmo, *How an iPhone Became the FBI's Public Enemy No. 1 (FAQ)*, CNET (Feb. 25, 2016, 4:00 PM), https://www.cnet.com/news/apple-versus-the-fbi-why-thelowest-priced-iphone-has-the-us-in-a-tizzy-faq.

[40] *Deleting data on Android devices after failed password entry attempts*, Kaspersky (last visited Jan. 30, 2025), https://support.kaspersky.com/help/KSMM/4.1/en-US/243163.htm.

Other common encryption workarounds applicable to E2EE generally fall into two categories. The first category is facilitatory variations on the brute-force attack, making such attacks easier by combining that blunt method with degrees of educated guesswork. For example, because about four percent of American smartphone users have "1234" as their passcode it makes sense to begin a brute-force attack there. Birthdates are another commonly used passcode. Such systematic guesswork has been successful in the past.[41, 42]

The second category encompasses workarounds which, despite being undeniably effective, are also sufficiently isolated or implausible as to prevent them being used on a wide-enough scale to be considered substantive solutions to E2EE's technical challenge.

Consider the striking example of the arrest of Ross Ulbricht, who ran an illegal drug market on the dark web in the early 2010s.[43, 44] FBI agents wanted to bypass the encryption on Ulbricht's laptop computer.

[41] *Id.*

[42] *See U.S. v. Lopez*, No. 13CR2092 WQH, 2016 WL 7370030 (S.D.Cal. Dec. 20, 2016).

[43] Press Release, U.S. Immigr. & Customs Enforcement, Ross Ulbricht, aka Dread Pirate Roberts, sentenced to life in federal prison for creating, operating 'Silk Road' website (May 29, 2015), https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating.

[44] Ulbricht received a "full and unconditional" federal pardon on January 21, 2025. *See* Nate Raymond, *Trump pardons Silk Road founder Ross Ulbricht for online drug scheme*, REUTERS (Jan. 22, 2025, 11:17 AM), https://www.reuters.com/world/us/trump-pardons-silk-road-founder-ulbricht-online-drug-scheme-2025-01-22/.

Knowing he was using the computer at a public library, two undercover agents casually approached Ulbricht. They then pretended to be a couple having a fight. When the fake fight distracted Ulbricht, the agents grabbed his still-open laptop, gave it to a colleague nearby, and then arrested Ulbricht. Because the laptop was, and remained, open during the whole incident, all the contents of its hard drive were completely decrypted.[45] The FBI's strategy in this case would certainly allow for law enforcement to review decrypted E2EE messages. But since it was wholly dependent on the factual circumstances of Ulbricht's case, it is unlikely that the strategy, however cunning, could be replicated for a meaningful number of suspects.

In another case,[46] law enforcement secretly installed a keylogger[47] on a suspect's home computer, using it to retrieve his passwords and thus to decrypt their desired content. Nevertheless, broadly idiosyncratic methods such as these are unlikely to be consistently applicable to E2EE: Consider not only the sheer volume of data-in-motion that exists, but also the safeguards already in place to protect that data. For example, logging back into Telegram after logging out permanently deletes all previous E2EE messages, users' ability to self-delete these messages notwithstanding.[48]

[45] Kerr & Schneier, *supra* note 26.
[46] United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).
[47] A piece of software which tells its operator every keyboard key that its subject presses.
[48] *Supra* note 2.

And WhatsApp, another popular messaging platform that uses E2EE, offers similar features.[49]

There is a common thread running through all of these methods of current practice, regardless of whether they are categorized as compelled decryption or alternative encryption workarounds: In a situation with E2EE, these methods would be conducted separately from the communication platform on which the E2EE messages were sent. The sole potential exception to this is a situation where the communication platform (upon receipt of a valid court order) provides law enforcement with an unencrypted or otherwise accessible backup of the desired content.[50] However, this is entirely a function of whether such a backup is available; if available, whether it is accessible; and if available and accessible, whether it is recent enough to contain the desired content. The significant emphasis placed upon privacy by platforms which offer E2EE and by E2EE's habitual users makes both of the first two conditions *very* unlikely.[51, 52, 53] In sum, it is apparent that social media and communication

[49] *About disappearing messages*, WhatsApp.com (last visited Jan. 31, 2025), https://faq.whatsapp.com/673193694148537.

[50] Kerr & Schneier, *supra* note 26 at 1010 - 1011.

[51] *Telegram Privacy Policy*, TELEGRAM.ORG (last visited Jan. 31, 2025), https://telegram.org/privacy.

[52] *About encrypted backups on your iPhone, iPad, or iPod touch*, Apple.com(last visited Jan. 31, 2025) https://support.apple.com/en-us/108353.

[53] *About end-to-end encrypted backup*, WhatsApp.com (last visited Jan. 31, 2025), https://faq.whatsapp.com/490592613091019.

platforms cannot adequately or reliably provide law enforcement with E2EE content. The question then becomes: Is that legal?

IV. The Stored Communications Act of 1986

A. Electronic Communication and Remote Computing Services

The Stored Communications Act (SCA)[54] creates an obligation on the part of any "provider of wire or electronic communication services (ECS) *or* a remote computing service (RCS)"[55] (emphasis added) to disclose certain information to governmental entities upon the government's valid and constitutional request.

Let us first turn to definitions. The SCA relies on the meanings of some terms defined by its contemporary statute, the Electronic Communications Privacy Act (ECPA) of 1986.[56] Among these definitions is that of an ECS: "Any service which provides to users thereof the ability to send or receive wire or electronic communications."[57] Electronic communications, meanwhile, are defined in the statute as including "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,

[54] Stored Communications Act, 18 U.S.C. 121 §§ 2701-2712 (2018).
[55] 18 U.S.C. § 2703(a).
[56] 18 U.S.C. § 2711(1) (2019).
[57] 18 U.S.C. § 2510(15) (2002).

electromagnetic, photoelectronic or photo optical system."[58] One intuitive example of ECS, supported by federal district and appellate case law, is email.[59]

The SCA defines RCS as "the provision to the public of computer storage or processing services by means of electronic communications system"[60] and incorporates the ECPA's definition of electronic communications system as any facilities or equipment for the transmission or storage of communications.[61] Email has also been considered as RCS under the SCA.[62] There is thus no reason why a service may not be both ECS and RCS; for example email is both because an email message itself is ECS while its storage is RCS.

Definitions aside, do the SCA's ECS and RCS terms apply to social media and other communication platforms as they are used today? The SCA, of course, became law in 1986—many years before the development of modern social media.

In *Crispin v. Christian Audigier, Inc.*, a federal district court held that Facebook (a service which uses E2EE today, but not at the time of the

[58] *Id.* at 12.
[59] *See generally* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2004); *see also* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (S.D.N.Y. 2008).
[60] 18 U.S.C. § 2711(2) (2019).
[61] 18 U.S.C. § 2510(14) (2002).
[62] U.S. v. Weaver, 636 F.Supp.2d 769, 770 (C.D.Ill.2009).

court's decision) and MySpace were social networking services that constituted ECSs under the SCA.[63] The operating principle in *Crispin* was that whether a service was an ECS or not depended upon whether it provided private messaging.[64] This 2010 case was the first in which the SCA's ECS and RCS definitions were applied to modern social media.[65] As has been discussed previously, it is difficult to conceive of any messaging *more* private than that provided by services which have E2EE enabled.

Crispin also clarified the scope of RCSs, holding that Facebook and MySpace were also RCSs because they (remotely) stored user messages that had been opened but not deleted, and that the recipients of such messages were thus using a remote computing service.[66] This interpretation proceeds from a different federal district court case, *U.S. v. Weaver*,[67] in which the court emphasized that the legislative intent behind the SCA was that when platforms stored any opened message that users had received, that "such communication should continue to be covered by section 2702(a)(2) [the section of the SCA which governs RCSs]."[68] This functionality is clearly present in service providers offering E2EE

[63] Crispin v. Christian Audigier, Inc., 717 F.Supp.2d 965, 982 (C.D.Cal. 2010).
[64] *Id*. at 980.
[65] *Id.* at 977 n.24, 982 n.35.
[66] *Id*. at 985.
[67] *Weaver*, 636 F.Supp.2d.
[68] *Id*. at 773, quoting H.R. REP. No. 99-647, at 65 (1986).

messaging. Otherwise, no one would actually be able see any messages which they had received—they would be instantly deleted upon receipt.

The case law is not unanimous on this issue, however. For example, last year in *Snap, Inc. v. Superior Court of San Diego County*,[69] the California 5th District Court of Appeal held that social media companies were not ECSs or RCSs.[70] The operating principle was based on the business model of the social media companies, Snap and Meta (Facebook's parent company, whose branding it still uses), in question: essentially, because Snap and Meta gave themselves the right to mine the contents of ostensibly private messages to offer users personalized sponsored advertisements, the messages were not truly private, and this storage was *not* offered for sole purpose of the provision of RCSs.

The Supremacy Clause notwithstanding, the operating principle in *Snap, Inc.* is unlikely to be applicable to social media companies in their particular roles as providers of E2EE messaging. Consider the technical impossibility of mining such messages (recall that communication platforms are not privy to the E2EE content they host). Meta explicitly acknowledges these limitations, while also noting that only some

[69] The plaintiff in this case is the manufacturer of the popular app Snapchat.
[70] Snap, Inc. v. Superior Court of San Diego County, 103 Cal.App.5th 1031 at 1062-1063 (2024).

ostensibly private messages are actually E2EE.[71] Snap, Inc.'s Snapchat, on the other hand, does not even provide E2EE on its popular text messaging service.[72], [73] The limitations caused by the technical impossibility E2EE induces would necessarily prevent any "business model" purpose from being applied to the platforms' storage.

Therefore, social media platforms *in their specific roles* as E2EE providers are ECSs and RCSs under the terms of the SCA. Governmental entities may, with a valid court order, require from such entities "the contents of a wire or electronic communication… [which are] in electronic storage in an electronic communications system."[74] Recall the SCA and ECPA's definition of electronic communications, stated at the beginning of this subsection. It should be clear that modern E2EE content constitutes electronic communication—the two "ends" of E2EE imply a transfer from one "end" to the other—regardless of the nature of that content itself. Recall that the term E2EE is most properly applied to data-in-motion.

[71] *End-to-end encryption*, Facebook.com (last visited Jan. 31, 2025), https://www.facebook.com/help/messenger-app/1084673321594605.
[72] Snapchat calls this service its "chats" feature.
[73] *Snapchat Security Essentials: Safeguarding Your Online Presence*, VeePN Research Lab (Aug. 14, 2024), https://veepn.com/blog/snapchat-security/.
[74] 18 U.S.C. § 2703(a) (2019).

B. Electronic Communication and Remote Computing Services

Applying the SCA's concept of electronic storage to E2EE content requires greater analysis. Do communication platforms, in their particular role as providers of E2EE, properly "store" E2EE content, considering the technical impossibility of their access to that content? The answer appears to be yes. Consider another post office analogy: I can have the post office hold my mail while I'm on vacation; assuming they do not open it, they store my mail without being privy to its contents. In computer science terms, the E2EE data is transmitted and stored (as will be explained below) on the host platform's servers without being decrypted.[75]

Recall too the court's holding in *Crispin* concerning the RCS status of Facebook and MySpace—storage was indeed present.[76] *Crispin* then proceeds to make the implicit explicit in its referencing of the ECPA, noting two *disjunctive* criteria enabling a type of storage to be considered "electronic storage" under the meaning of the SCA. First, that the storage is "temporary and intermediate"; or second, that it is for backup purposes.[77] The existence of these two criteria, as well as their disjunctive quality, was

[75] *Supra* note 15.

[76] *Christian Audigier, Inc.*, 717 F.Supp.2d at 985.

[77] *Id*. at 973, quoting 18 U.S.C. § 2510(17) (2002).

corroborated in the federal appellate decision in *Garcia v. City of Laredo, Tex.*[78]

Let us now consider what makes a type of storage "temporary and intermediate." First, *Crispin* drew upon another federal district court case, *Snow v. DIRECTV, Inc.*,[79] to set forth the operative principle for determining whether storage is "temporary and intermediate." To paraphrase the court's holding in *Snow*, if certain content cannot be deleted by the platform or stored as a message until it has been opened, then that content experiences temporary, intermediate storage.[80] This, of course, applies to E2EE content—recalling that the two "ends" of E2EE each need to open each other's content before seeing it.

If that were not enough to consider E2EE content as electronically stored under the meaning of the SCA, it is also true that many of the more popular communication platforms which offer E2EE also offer cloud backup services.[81] These backup services are *themselves* under E2EE,[82, 83] which carries all the accompanying restrictions. In this way, E2EE content

[78] Garcia v. City of Laredo, Tex., 762 F.3d. 788 at 793 (5th Cir. 2012).

[79] *Snow v. DIRECTV, Inc.*, 2005 WL 1226158 at *1 (M.D. Fla. May 9, 2005).

[80] *Christian Audigier, Inc.*, 717 F.Supp.2d at 988.

[81] A cloud backup service is one which stores encrypted data to a remote "cloud-based" server administered by a "third-party cloud service provider." *See Cloud Backup*, OpenText.com (last visited Feb. 17, 2025), https://www.opentext.com/what-is/cloud-backup.

[82] *Supra* note 53.

[83] *Turn on secure storage for end-to-end encrypted messages*, Facebook.com (last visited Feb. 1, 2025), https://www.facebook.com/help/messenger-app/820525008940780.

also fits perfectly the second criteria of electronic storage set forth in the statutory and case law.

The heart of the inconsistency between current E2EE practices and communication platforms' obligations to disclose under the SCA is now hopefully apparent. Assuming the existence of a valid, constitutional court order (an assumption whose validity is outside this Article's scope), communication platforms *must* be able to disclose E2EE content to law enforcement. But even upon receipt of such an order, the platforms' inability to access this content, which is nevertheless in their electronic storage, prevents disclosure. To sum up, platforms which use E2EE are incapable of complying with the SCA. A question thus presents itself: Is there any legal mechanism for communication platforms to extricate themselves from this apparently tricky situation?

V. THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT OF 1994

The Communications Assistance for Law Enforcement Act (CALEA)[84] sets forth the "duty of telecommunications carriers [TCs] to cooperate in intercepting communications for law enforcement purposes"

[84] The Communications Assistance for Law Enforcement Act of 1994, 47 U.S.C. §§ 1001-1010 (1994).

as well as the exceptions to it.[85] Of particular interest is Section 1002 of CALEA, which explains the accessibility requirements that the government imposes on such TCs.[86] These requirements are less stringent than those which the SCA imposes on ECSs and RCSs, and *if* providers of E2EE are considered TCs, then CALEA's encryption carve-out[87] would potentially (putting aside the resulting conflict of laws) free E2EE providers from their obligations to disclose under the SCA.

As with our discussion of the SCA, we must first consider the issue of definitions. What exactly are TCs? And are social media and communication platforms considered TCs under CALEA? The statute defines TC as "a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire."[88] CALEA *excludes* from its definition of TC "…entities insofar as they are engaged in providing information services."[89] The definition that the statute provides for "information services" is verbose and not particularly useful: "the offering of a capability for generating, acquiring, storing, transforming,

[85] 68 Am. Jur. 2d *Searches and Seizures* § 350 (2025).
[86] 47 U.S.C. § 1002.
[87] *Id*. at (b)(3).
[88] 47 U.S.C. § 1001(8).
[89] *Id*.

processing, retrieving, utilizing, or making available information via telecommunications."[90]

Nonetheless, CALEA provides a helpful further clarification by explicitly including "electronic messaging services" within "information services."[91] Recall, of course, that E2EE is most commonly, closely and appropriately applied to the *data-in-motion* generated by such electronic messaging services—Telegram, WhatsApp, Facebook, etc.

While this interpretation is ostensibly straightforward, the technological fuzziness of these concepts cry out for clarification from the case law. In *American Council on Educ. v. F.C.C.*, a federal appellate court, ruling that broadband providers were TCs, stated explicitly that information services are not subject to CALEA[92] and that the FCC was reasonable in distinguishing between them.[93] In sum, social media companies and communication platforms in their particular roles as providers of E2EE messaging services are not considered to be TCs under CALEA—precisely because they provide such messaging services.

This is significant because, at first glance, CALEA would seem to provide a way for these platforms to escape the technical SCA violation

[90] *Id.* at 6.
[91] *Id.*
[92] American Council on Educ. v. F.C.C., 451 F.3d 226, 228 (D.C. Cir. 2006).
[93] *Id*. at 234.

discussed in the last section. As mentioned above, section 1002(3) carves out an exception to the duty-to-cooperate mandated by CALEA, providing that "[a TC] shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer."[94] The operative phrase there is, of course, TC. This exception, then, does not apply to E2EE providers, and so they have no method of extrication from the problem set forth in this Article's previous section.

Nonetheless, there is an exception-within-the-exception that is worth exploring for clarity and thoroughness's sake. Section 1002(3) immediately follows the preceding rule with "…unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."[95] Even if E2EE providers were TCs, they would meet the first condition while failing to meet the second. The end result would be that they would not be responsible for decryption, rendering any disclosed encrypted content totally useless. The consequent lack of responsibility *could* help alleviate E2EE providers from the SCA's burden, but it fails to do so because the providers are definitely *not* TCs, as this section establishes.

[94] 47 U.S.C. § 1002(3).
[95] *Id*.

VI. The All Writs Act of 1789

Despite the technologically-intricate setting, a law as old as the All Writs Act (AWA)[96] has become increasingly relevant in the face of the general challenge encryption poses to law enforcement. The relevant text of the statute itself is brief: "The Supreme Court and all courts established by Act of Congress may issue all writs [a court's written order commanding the recipient to do or not do some specific action][97] necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[98] The three discretionary criteria are that (1) the writ must be in aid of the court's jurisdiction; (2) that the writ is necessary and appropriate to do so; and (3) that the writ is "agreeable to the usages and principles of law."[99] This intentionally indefinite phrase serves to place the writ's issuance squarely within the court's discretion.[100] Finally, case law has further and unambiguously indicated that the writ's issuance is a method of last resort.[101]

[96] The All Writs Act of 1789, 28 U.S.C. § 1651 (1949).

[97] *Writs*, BLACK'S LAW DICTIONARY (12th ed. 2024).

[98] 28 U.S.C. § 1651(a).

[99] *In re Apple, Inc.*, 149 F.Supp.3d 341, 350 (E.D.N.Y. 2016), citing 28 U.S.C. § 1651(a) (1949).

[100] *See generally Id.* at 350-351.

[101] John L. Potapchuk, *A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data Under the All Writs Act*, 57 B.C. L. REV. 1403, 1422 (2016), citing Brown v. Gilmore, 533 U.S. 1301, 1303 (2001) and Ohio Citizens for Responsible Energy, Inc. v. Nuclear Regul. Comm'n., 479 U.S. 1312, 1313-14 (1986). *See* Clinton v. Goldsmith, 526 U.S. 137, 139 (1999).

The cumulative judicial interpretations of the criteria above have created a situation whereby law enforcement can use the AWA to compel third-party assistance in retrieving content. Doing so requires that a valid search warrant has previously been issued for the desired content. This helps fulfill the first of the three discretionary criteria discussed above: the writ compels the third-party to allow the warrant to be enforced, and the enforcement of the warrant is what makes the writ's issuance "in aid of the court's jurisdiction."

This was precisely the logic used in the Supreme Court's decision in *U.S. v. New York Tel. Co.*,[102] a case which allowed the use of the AWA to compel third parties to assist law enforcement generally—here, to allow the FBI to install a phone number logger on one of the New York Telephone Co.'s telephones. This case accordingly provides the legal precedent for the AWA's interpretation and usage in the context of compelled decryption.[103] *New York Tel. Co.* also imposed a further condition upon courts issuing AWA writs, requiring that they are not "unreasonably burdensome" (yet

[102] United States v. New York Telephone Co., 434 U.S. 159 (1977). The specifically technological relevance of this case has, of course, diminished considerably in the almost-fifty years since it was decided.

[103] Cyrus Farivar, *Apple tells court it would have to create "GovtOS" to comply with ruling*, Ars Technica (Feb. 25, 2016, 3:03 AM), https://arstechnica.com/tech-policy/2016/02/apple-fires-back-at-doj-this-is-not-a-case-about-one-isolated-iphone/.

another phrase which serves to amplify the court's discretionary power) upon the compelled provider of assistance.[104]

The most important recent (ten years old, but very much initiating a trend) development in the AWA case law is *In re Order Requiring Apple Inc., to Assist in the Execution of a Search Warrant Issued by This Court* (*In re Apple, Inc.* for short),[105] in which a federal magistrate judge denied the government's request to compel Apple to unlock a suspect's iPhone. The reason was the court's reluctance to infringe upon Congressional prerogative. Congress had previously considered, but failed to adopt, legislation covering these kinds of compelled decryption practices; therefore, it would not have been "agreeable to the usages and principles of law" to permit the government's request in this instance.[106] Note that this case does not strictly implicate E2EE; the government's request here was for a proxy-key workaround to symmetric encryption that was protecting data-at-rest.[107] Subsequent developments in the case law, even at their most variable in comparison to *In re Apple, Inc.*, have not expanded the AWA in a way that would easily facilitate similar government requests.[108]

[104] *New York Tel. Co.*, 434 U.S. at 172.

[105] *In re Apple, Inc.*, 149 F.Supp.3d.

[106] Potapchuk, *supra* note 101 at 1422, quoting *In re Apple, Inc.*, 149 F.Supp.3d at 353, 360-1, 363-4 (E.D.N.Y. 2016).

[107] *Supra* note 24.

[108] *See generally Matter of U.S.*, 256 F.Supp.3d 246 (E.D.N.Y. 2017); *see also Forbes Media LLC v. U.S.*, 61 F.4th 1072 (9th Cir. 2023).

Now that we have a basic understanding of the AWA and its interpretation, the key question becomes whether the AWA would allow E2EE providers any relief from the previously discussed inconsistency between current practices and the SCA's law. The answer must be no. The simple fact of (asymmetric) E2EE is that the communications platform hosting E2EE content would be technologically incapable of providing the sort of assistance required under the AWA—recall from Section I of this Article that the hosting platform is simply not privy to the content they are supposed to be disclosing.

So, no court is likely to issue an AWA writ against an E2EE provider. While the issuance might be in aid of the court's jurisdiction by enforcing a previous court order, the issuance would be an inappropriate method of doing so. And it is not merely unreasonably burdensome, but a technologically insurmountable imposition upon E2EE providers to compel their assistance in decrypting E2EE content.

Interestingly, this rationale is somewhat paralleled in the circumstances which led Apple to litigate *In re Apple, Inc.* in the way that it did. Even ten years ago, the technological sophistication of Apple's methods for symmetrically encrypting data-at-rest would have essentially prevented it from complying with the AWA without imposing an "unreasonable" burden under *New York Tel. Co.*[109] Today's methods, meanwhile, leave "burdensome" behind and approach technical impossibility—recall the brief discussion of AES-XTS encryption in Section II of this Article.

Ultimately, if there is no plausible issuance, then the AWA imposes no obligations on E2EE providers, but neither does it relieve providers of their burden under the SCA. The technical characteristics of E2EE and the elements of the AWA prevent that statute from touching E2EE providers in any meaningful way whatsoever. Indeed, there is no indication in the case law that the AWA has been applied specifically to E2EE—which stands in relative contrast to how the SCA's definitions *do* logically apply to it. Certainly, a court's case-by-case discretionary refusal to grant a demand under the AWA for technological assistance, borne solely out of *very* recent developments in the case law, must carry less weight than the SCA's explicit, codified obligation to disclose. But in any case, *neither* CALEA nor AWA would seem to provide relief to E2EE providers from the problematic inconsistency created by the SCA and current E2EE practices.

[109] Potapchuk, *supra* note 101 at 1435.

VII. Conclusion

In the contest between the relentless forward-march of technological progress and a doddering, outdated statute, it is not immediately clear that the latter should prevail simply by virtue of being the law. The SCA's problematic nature is very well known. Even *Crispin*, and a conceptually-related federal appellate decision, both[110] note the difficulty of statutory interpretation in a situation where the applicable statute significantly predates the Internet—and social media—in their modern and most widely used forms. Stronger phrases, such as "ill-suited for modern technology"[111] and "hopelessly outdated",[112] have also been applied. The present state of warrantless disclosure of some non-E2EE geolocation data as required by the SCA has even been ruled unconstitutional because such disclosure violates a suspect's right to privacy under the Fourth Amendment.[113, 114]

In stark contrast, encryption technologies, including E2EE, are now progressing at an incomprehensible speed. For example, one of the latest

[110] *Christian Audigier, Inc.*, 717 F.Supp.2d at 988, quoting *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002).
[111] Richard McCutcheon, *Impractical and Unconstitutional: The Stored Communications Act Post-Carpenter*, HARV. NAT'L. SEC. J. ONLINE (Oct. 17, 2024).
[112] Melissa Medina, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267, 287 (2013).
[113] McCutcheon, *supra* note 111.
[114] *See generally Carpenter v. U.S.*, 585 U.S. 296 (2018).

research developments is to create quantum-proof encryption algorithms that cannot even be successfully brute-force attacked by quantum computers. These are computers that, apparently, operate according to the laws of quantum physics rather than to those of classical physics—and accordingly possess significantly greater computational power.[115]

Other developments include the concept of "homomorphic encryption", which would allow calculations to be performed on data without decrypting it.[116] The wide-scale implementation of homomorphic encryption would create *more* situations roughly similar to E2EE. Users' preference for privacy would popularize platforms that provide homomorphically encrypted data services over platforms which provide identical but unencrypted data services. For the government to try and stop these tides of progress while maintaining a stagnant legislative framework would be unwise, unpopular, and futile. Both the government and the public benefit from stronger encryption, as far as their own protection from cybercriminals is concerned, and consumers have made clear their taste and preference for increasing levels of privacy and security online.

[115] A. Sizensky, *The Future of Encryption: Advancements and Challenges*, Tech Blogs by SAP (Jan. 5, 2024, 10:39 AM), https://community.sap.com/t5/technology-blogs-by-sap/the-future-of-encryption-advancements-and-challenges/ba-p/13574094.
[116] *Id.*

At the same time, it does not serve the public interest to allow suspected criminals to operate without fear of detection or apprehension so long as they take sufficient care in encrypting their data. If an attack on the progress of cryptographic science is off the table, then ultimately, a comprehensive legislative solution of some kind will eventually be needed; the judiciary can only plug the gap for so long. Regardless of how Congress chooses to precisely strike the crucial balance between consumer privacy and public safety, it should explicitly clarify platforms' legal obligations to law enforcement in light of the most recent developments in encryption technology. At the very least, the law should be sufficiently up-to-date and adaptable so as to not impose technologically impossible requirements on communication platforms while simultaneously failing to promote public safety. Unfortunately, the law as it currently exists has failed to meet even these basic conditions.