Don't Kill the Messenger: How the New Technologies Used by Internet-Based Communications Providers are Gutting Compelled Disclosure Laws

By Veronika Balbuzanova

INTRODUCTION……..……..1
I. FEDERAL LAWS PROVIDING FOR COMPELLED DISCLOSURE OF ELECTRONIC COMMUNICATIONS……2
II. SECURITY FEATURES AIMED AT PREVENTING UNAUTHORIZED ENTRY INTO USERS' ACCOUNTS AND DEVICES……..……..7
A. *Guarding Against Government Access to One's Device*……..…...……..7
B. *Guarding Against Government Access to One's Account: Two-Factor Authentication*……...…….. 9
III. SECURITY PROGRAMS TAILORED TO ELIMINATING UNAUTHORIZED ACCESS TO USERS' ELECTRONIC COMMUNICATIONS……..10
A. *The Statutory Framework*…...……..22
B. *End-to-End Encryption*……..10
C. *Ephemeral Communications*.……..…….……....15
IV. LIKELY OUTCOMES AND VIABLE SOLUTIONS TO THE GOING DARK PROBLEM……...…….....23
V. CONCLUSION……..……....17

INTRODUCTION

A roaring revolution has taken place in the social media world and law enforcement has gotten the short end of the stick.[451]

There used to be a time when electronic communications providers sacrificed their users' privacy concerns for their own financial gain.[452] Email providers routinely used complex algorithms to scan and analyze the contents of their users' incoming and outgoing messages in order to tailor advertisements to each user's unique preferences.[453] In turn, email providers gained a substantial percentage of their revenue from selling these targeted advertisements to companies and businesses interested in marketing their products online.[454] In recent years, however, a growing number of popular messaging applications have flipped the script on their use of technology altogether.[455] The privacy of their users' communications has become the foundation of their companies, and the technological innovations they employ have solidified that foundation.[456] In the words of one such messaging app, "Respect for your privacy is coded into our DNA."[457]

---

[451]. *See* Matt Apuzzo, *WhatsApp Encryption Said to Stymie Wiretap Order*, N.Y. TIMES (Mar. 12, 2016), https://www.nytimes.com/2016/03/13/us/politics/whatsapp-encryption-said-to-stymie-wiretap-order.html; Brett Max Kaufman, *New Documents Reveal Government Effort to Impose Secrecy on Encryption Company*, ACLU (Oct. 4, 2016, 7:00 AM), https://www.aclu.org/blog/national-security/secrecy/new-documents-reveal-government-effort-impose-secrecy-encryption.

[452]. *See In re* Yahoo Mail Litig., 7 F. Supp. 3d 1016, 1021 (N.D. Cal. 2014).

[453]. *Id.*

[454]. *Id.* Yahoo's annual revenue from such advertising was as high as seventy-five percent. *Id.*

[455]. *See, e.g.*, Vivienne Walt, *With Telegram, a Reclusive Social Media Star Rises Again*, FORTUNE (Feb. 23, 2016, 4:25 AM), http://fortune.com/telegram-pavel-durov-mobile-world-congress/. However, some communications providers still routinely scan and analyze the contents of their users' messages in order to provide targeted advertisements. *Yahoo Privacy Center*, YAHOO!, https://policies.yahoo.com/us/en/yahoo/privacy/index.htm (last updated June 13, 2017). Yahoo's Privacy Policy states that it collects such information "to customize the advertising and content you see." *Id.* Likewise, Facebook's Terms of Service state that, in utilizing Facebook's services, users agree to give Facebook access to the content of their communications, so the company can "deliver advertising and other commercial or sponsored content that is valuable to our users and advertisers." *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/terms.php (last revised Jan. 30, 2015). Snapchat also personalizes ads according to information it collects from users' use of the application, though such information does not include the actual content of the messages. *Privacy Policy*, SNAP, INC., https://www.snap.com/en-US/privacy/privacy-policy/ (last modified June 5, 2017).

[456]. *See Privacy Policy*, *supra* note 5; *Security Practices*, SLACK (May 24, 2018), http://slack.com/security-practices; *End-to-End Encryption*, WHATSAPP: FAQ, http://faq.whatsapp.com/en/android/28030015/ (last visited Sept. 10, 2018).

[457]. *WhatsApp Privacy Policy*, WHATSAPP, http://www.whatsapp.com/legal/#privacy-policy (last modified Aug. 25, 2016).

Innovations in technology have given rise to new security features and programs which preserve and protect users' privacy at various stages in the communication process.[458] In order to protect the user from unauthorized entry into his account or device, companies are incorporating encrypted passwords and two-factor authentication.[459] To prevent unauthorized access to the contents of messages, technologies such as end-to-end encryption and ephemeral communications are being employed.[460] While these security measures protect users from traditional hackers, such technological innovations also have the effect of preventing law enforcement agents from obtaining access to information that they otherwise have the legal and statutory authority to obtain.[461] This dilemma is referred to as the "going dark" problem ("Going Dark Problem").[462] Even after complying with legal requirements and following proper procedures, agents must still overcome the roadblock that these innovations place in their path.[463]

This Comment will discuss the Going Dark Problem faced by law enforcement and the viability of the different solutions available to state and federal authorities.[464] Specifically, this Comment will analyze the use of security features by Internet-based Communications Providers ("ICPs")—"email, Internet messaging, social networking sites, [and] peer-to-peer services."[465] Since there are many companies which fall under this definition of an ICP, only some of the most popular ones will be discussed—

458. *See* Walt, *supra* note 5.
459. *Security Practices*, *supra* note 6.
460. Walt, *supra* note 5; *Privacy Policy*, *supra* note 5.
461. Apuzzo, *supra* note 1.
462. *Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, before the S. Comm. On the Judiciary, 114th Cong. (Jul. 8, 2015) (statement of Sally Quillian Yates and James B. Comey).
463. *Id.*; Apuzzo, *supra* note 1.
464. *See infra* Part IV–V.
465. *Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, *supra* note 12.

Snapchat,[466] WhatsApp,[467] Slack,[468] Signal,[469] Telegram,[470] ProtonMail,[471] and certain privacy features provided by Apple.[472] Part II of this Comment will provide a brief overview of federal laws which compel various types of communications providers to disclose their users' communications to law enforcement.[473] This Comment will then explore the security features associated with entry into a user's messaging account or device.[474] Subsequently, Part IV will discuss the two main security programs used by apps to protect the contents of messages.[475] Part V will propose two viable solutions to the Going Dark Problem: (1) improving and developing the government's own use of communications technologies; and (2) amending the Stored Communications Act ("SCA") to provide for preservation requests of future communications.[476]

I. FEDERAL LAWS PROVIDING FOR COMPELLED DISCLOSURE OF ELECTRONIC COMMUNICATIONS

When it comes to compelled disclosure of users' communications by ICPs, there are several federal statutes which address the topic either directly or indirectly.[477] The Electronic Communications Privacy Act ("ECPA") of 1986 directly addresses the proper guidelines that law enforcement agents must follow in order to legally compel

---

[466]. *What is Snapchat?*, SNAP, INC., http://whatis.snapchat.com/ (last visited Sept. 10, 2018). Snapchat, Inc. characterizes itself as "a new kind of camera," whereby users can send either private or group photos, videos, and messages to others. *Id.*

[467]. WHATSAPP, http://www.whatsapp.com/ (last visited Sept. 10, 2018). WhatsApp is an ICP that provides messaging and calling services to users around the world. *Id.*

[468]. *Why Slack?: How It Works*, SLACK, http://slack.com/features (last visited Sept. 10, 2018). Slack is uniquely tailored to communication among colleagues in the workplace, featuring voice and video calls, integrated file sharing, and channels and threads for messaging. *Id.*

[469]. SIGNAL, http://signal.org/ (last visited Sept. 10, 2018). Signal allows users to send free "high-quality group, text, voice, video, document, and picture messages" to others around the world. *Id.*

[470]. TELEGRAM, http://telegram.org/ (last visited Sept. 10, 2018). Telegram is a free messaging app that allows users to send messages and files using different levels of encryption. *Id.*

[471]. PROTONMAIL, http://protonmail.com/ (last visited Sept. 10, 2018). ProtonMail is a free, open source, encrypted email provider incorporated in Switzerland. *Id.*

[472]. *Legal Process Guidelines*, APPLE (Aug. 16, 2018), http://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; *About Touch ID Advanced Security Technology*, APPLE: SUPPORT, http://support.apple.com/en-us/HT204587 (last visited Sept. 10, 2018). Apple is the technology giant that "designs, manufactures, and markets mobile communication and media devices." *Legal Process Guidelines*, *supra*.

[473]. *See infra* Part II.

[474]. *See infra* Part III.

[475]. *See infra* Part IV.

[476]. *See infra* Part V.

[477]. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2712, 3121–3127 (2012); All Writs Act, 28 U.S.C. § 1651 (2012).

ICPs to turn over both the content and non-content data of its users.[478] Much of these guidelines are housed in the SCA, which is part of the ECPA.[479]

In contrast, the All Writs Act is not a statute that is specific to the compelled disclosure issue or to ICPs.[480] Rather, its general language can be applied and used to assist law enforcement agents in accessing customer data that they otherwise have the legal right to access.[481] Additionally, the Communications Assistance for Law Enforcement Act ("CALEA") provides insight into the possible future of compelled disclosure laws despite its current inapplicability to the ICPs discussed in this Comment.[482] As its name suggests, CALEA is intended to aid law enforcement agents in conducting their investigations by requiring telecommunications carriers to have the proper means available to intercept or access call-identifying information.[483] A telecommunications carrier is defined as "a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire."[484] CALEA states that telecommunications carriers must be capable of "expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier. . . ."[485] This requirement also extends to certain call-identifying information.[486]

II. SECURITY FEATURES AIMED AT PREVENTING UNAUTHORIZED ENTRY INTO USERS' ACCOUNTS AND DEVICES

Although this Comment explores the security features being incorporated specifically into messaging applications, the fact that users use devices to access their apps cannot be ignored.[487] For that reason, a brief discussion of the features available to protecting one's device from unauthorized entry is included.[488] That discussion

---

478. § 2703.
479. Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012).
480. *See* 28 U.S.C. § 1651.
481. *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, No. 1:15-mc-01902-JO, 2015 WL 5920207, at *1 (E.D.N.Y. Oct. 9, 2015).
482. *Id.* at *2. "However, CALEA's requirements did not cover electronic mail, instant messaging, peer-to-peer communications, or social media." *Id.*
483. Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001–1010 (2012).
484. *Id.* § 1001(8).
485. *Id.* § 1002(a)(1).
486. *Id.* § 1002(a)(2).
487. *About Touch ID Advanced Security Technology*, *supra* note 22.
488. *See infra* Part III Section A.

includes a look at a popular security option used to guard against unauthorized entry of one's ICP account.[489]

A. Guarding Against Government Access to One's Device

The next best thing to having no one access your personal data and communications is having only those entities that you authorize to access your data, do so.[490] Typically, that involves creating a barrier in the form of a password.[491] While users always have the option of resorting to the typical alphanumeric password, they may also take their security measures a step further by adding a fingerprint passcode.[492] For owners of Apple devices, this would entail using the Touch ID feature on their iPhones, which first requires the creation of an alphanumeric password followed by a fingerprint scan.[493] Using both of these security measures makes for a practically hackproof device.[494] The image of the fingerprint is never stored.[495] Rather, a mathematical representation is retained and protected by the Secure Enclave, an *advanced security architecture* that makes it impossible for anyone to reverse-engineer the mathematical representation into the fingerprint image.[496] That data—the mathematical representation—is encrypted and never backed up to servers or the iCloud.[497] Text messages, photos, videos, and files sent through iMessage are likewise (end-to-end) encrypted.[498]

Encryption is a process by which regular data—anything from the contents of messages to mathematical fingerprint representations and passwords—is scrambled in order to become incomprehensible gibberish to anyone intercepting it.[499] The regular, or unencrypted, data is commonly referred to as plaintext; the scrambled, or encrypted, data is also known as cyphertext.[500] An encryption algorithm and key is required to unscramble the cyphertext back into recognizable words, photos, files, etc.[501]

---

489. *See infra* Part III Section B.
490. Nadeem Unuth, *What Is End-to-End Encryption?*, LIFEWIRE, http://www.lifewire.com/what-is-end-to-end-encryption-4028873 (last updated Sept. 5, 2018).
491. *About Touch ID Advanced Security Technology*, *supra* note 22.
492. *Id.*
493. *Id.*
494. *Id.*
495. *Id.*
496. *About Touch ID Advanced Security Technology*, *supra* note 22.
497. *Id.*
498. *Legal Process Guidelines*, *supra* note 22.
499. Unuth, *supra* note 40.
500. *Id.*
501. *Id.*

There is a sad irony when it comes to controlling the government's—as opposed to any regular hacker's—access to one's device.[502] The use of fingerprint passcodes provides greater security protections from individuals attempting to access a user's device.[503] While the probability of someone guessing a four-digit password is one in ten thousand, the odds of someone finding a different fingerprint that would be similar enough to trigger a fingerprint match are one in fifty thousand.[504] Despite the greater protection that fingerprint passcodes provide against typical hackers, the exact opposite is true when law enforcement is the one accessing the device.[505] Users have greater legal protections when they are compelled to disclose alphanumeric passwords to authorities than when they are compelled to provide their fingerprints to unlock fingerprint passcodes.[506]

Courts have held that compelling an individual to disclose his alphanumeric password to authorities implicates the Fifth Amendment because the individual must use his knowledge and mental processes to provide the password.[507] In contrast, providing a fingerprint is a type of physical characteristic evidence, which is not subject to Fifth Amendment protections.[508] Furthermore, the government may overcome the implication of Fifth Amendment protections regarding the compelled disclosure of an alphanumeric password if the government satisfies the elements of the foregone conclusion doctrine.[509] The underlying rationale of the doctrine is that, even though providing a password involves the use of one's mental thoughts and processes, disclosing the password is not protected where it does not carry testimonial significance.[510] The production of a password is not testimonial where law enforcement authorities show, with reasonable particularity, the *existence, possession, and authenticity* of the information.[511] In other words, the production of the password would not add anything to the government's case or incriminate the accused because law enforcement authorities "already knew the evidence sought existed, the evidence

---

[502]. *See* State v. Stahl, 206 So. 3d 124, 135 (Fla. 2d Dist. Ct. App. 2016).

[503]. *About Touch ID Advanced Security Technology*, *supra* note 22.

[504]. *Id.*

[505]. *See* Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014).

[506]. *Id.*

[507]. *Id.*

[508]. *Id.*

[509]. *Stahl*, 206 So. 3d at 135.

[510]. *Id.* at 133-34. The Fifth Amendment provides that no person "shall be compelled in any criminal case to be a witness against himself…." U.S. CONST. amend. V. For a Fifth Amendment privilege to be implicated, the accused must prove that the information to be disclosed or produced is incriminatory, compelled, and testimonial. *Stahl*, 206 So. 3d at 131. The foregone conclusion doctrine, when satisfied, proves that the last element—a testimonial communication—has not been met. *See Id.* at 132.

[511]. *Stahl*, 206 So. 3d at 135.

was in the possession of the accused, and the evidence was authentic."[512] The *evidence* refers to the password itself, not the contents on the device that the government seeks to obtain.[513]

Though the foregone conclusion doctrine has been used to compel the production of a password, its use in this manner has also been rejected and criticized by some courts.[514] A Virginia Circuit Court refused to compel the production of a passcode on the ground that if the password were really a foregone conclusion, then law enforcement agents would have already known it.[515] The fact that they did not, and that they had to resort to compelling its production from the defendant, was itself proof that the password was not a foregone conclusion.[516] Similarly, the Second District Court of Appeal of Florida criticized the greater Fifth Amendment protections given to password-protected devices as opposed to fingerprint-protected ones.[517]

Alternatively, law enforcement agents have turned to cellphone manufacturers to gain access to users' devices.[518] Pursuant to the All Writs Act, some courts have ordered manufacturers to assist agents in bypassing screen locks and passwords.[519] The All Writs Act—all fifty-three words of it—states:

> (a) The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.
>
> (b) An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction.[520]

The All Writs Act is typically used in conjunction with another statute to enable law enforcement to compel the disclosure of user data.[521] It is a *residual source of authority* that is intended to fill statutory gaps, not to establish a wholly new avenue for the government to obtain court orders.[522] Most notably, it has been used to compel

---

512. *Id.*
513. *Id.* at 136.
514. *See id.* at 135.
515. *Baust*, 2014 WL 10355635, at *4.
516. *Id.*
517. *Stahl*, 206 So. 3d at 135. "More importantly, we question the continuing viability of any distinction as technology advances." *Id.*
518. *See In re* Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant Issued by This Court by Unlocking a Cellphone, No. 14 Mag. 2258, 2014 WL 5510865, at *2 (S.D.N.Y. Oct. 31, 2014).
519. *Id.*
520. 28 U.S.C. § 1651.
521. *In re Order Requiring Apple, Inc. to Assist*, 2015 WL 5920207, at *1.
522. *Id.*

both users and service providers to either disclose data that is sought or to assist law enforcement in obtaining such data.[523]

Other courts, in contrast, have deferred ruling on the issue until they have determined whether complying with the assistance order would be technically feasible or unduly burdensome on the manufacturer.[524] Such courts have recognized that manufacturers' burdens go beyond those associated with financial costs and physical demands.[525] The highest burden they bear is making sense of the contradiction that arises when ICPs assist government officials in overriding their own privacy protections—protections they intentionally included in order to reflect the commitment to privacy implicit in their companies' privacy policies.[526]

B. Guarding Against Government Access to One's Account: Two-Factor Authentication

For an added layer of security, users can choose to enable two-factor authentication on ICP accounts that feature this option.[527] As the name suggests, two-factor authentication—or two-step verification—entails a two-step process to logging in to one's ICP account.[528] The first step is the username and password characteristic of most account log-ins.[529] The second step requires the input of some additional piece of identifying information, such as a verification code or security key.[530] The specific type of code or key varies with the app, as some may feature more options to choose from.[531] Typically, however, users may choose to either receive a text message with

---

523. *See infra* Part III.

524. *In re Order Requiring Apple, Inc. to Assist*, 2015 WL 5920207, at *1.

525. *Id.* at *6.

526. *Id.*

> The decision to allow consumers to encrypt their devices in such a way that would be resistant to ready law enforcement access was likely one that Apple did not make in haste, or without significant consideration of the competing interests of public safety and the personal privacy and data security of its customers. [Citation omitted]. It may reflect an analysis of Apple's business prospects that persuaded the company that failing to provide its customers with the kind of privacy protection the government now seeks to overcome would have long-term costs that outweighed the benefits of a technological approach more to the government's liking.

Id.

527. *Two-Factor Authentication*, SNAPCHAT: SUPPORT, http://support.snapchat.com/en-US/article/enable-login-verification (last visited Sept. 10, 2018).

528. *Id.*

529. *Id.*

530. *Id.*

531. *See What Is Two-Factor Authentication and How Does It Work?*, FACEBOOK: HELP CENTER, http://www.facebook.com/help/148233965247823 (last visited Sept. 10, 2018).

the security code directly from the ICP itself or from an authentication application of their choosing.[532]

Two-factor authentication provides additional security of one's account since someone that knows a user's password, but not their separate security code or key, would still be unable to log into the user's account.[533] Slack applies two-factor authentication when a user is logging in to their account, provided that the user has opted in to the feature.[534] Some ICPs, however, utilize two-factor authentication to something other than log-in attempts.[535] For example, WhatsApp applies it to any attempts to verify a user's phone number.[536] A user who opts in to Facebook, Snapchat, or Telegram's two-factor authentication must provide the additional security code whenever there is a login attempt from a new or unrecognizable device.[537] Regardless of the specifics of how each ICP uses the security feature, it nevertheless provides a further guarantee against unauthorized entry into one's account.[538] This is so especially if law enforcement agents have legally obtained a user's password and are attempting to log in to his account from a device that is not the one the user uses on a regular basis.[539] In that case, they would be prompted to enter the security code as part of the two-step authentication process—a code which they would not know without either having the user's device in their possession or obtaining the code itself from the user.[540]

The relationship between law enforcement and ICPs is not affected by two-factor authentication because there is no statutory provision that regulates the use of this feature.[541] Even where a user has opted in to two-factor authentication, law enforcement's power to compel production does not extend to production of a user's log-in credentials or direct access to the user's account, itself.[542] Thus, two-factor authentication is a security feature that gives users extra protection in a narrow set of

---

[532]. *See id.*

[533]. *Two-Factor Authentication*, *supra* note 77.

[534]. *See Mandatory Workspace Two-Factor Authentication*, SLACK, http://get.slack.help/hc/en-us/articles/212221668-team-wide-two-factor-authentication (last visited Sept. 10, 2018).

[535]. *See Two-Step Verification*, WHATSAPP, http://faq.whatsapp.com/en/general/26000021 (last visited Sept. 10, 2018).

[536]. *Id.*

[537]. *What Is Two-Factor Authentication and How Does It Work?*, *supra* note 81; *Two-Factor Authentication*, *supra* note 77; *Active Sessions and Two-Step Verification*, TELEGRAM (Apr. 8, 2015), http://telegram.org/blog/sessions-and-2-step-verification.

[538]. *Mandatory Workspace Two-Factor Authentication for Your Team*, *supra* note 84.

[539]. *See What Is Two-Factor Authentication and How Does It Work?*, *supra* note 81.

[540]. *See id.*

[541]. *See* 18 U.S.C. § 2703.

[542]. *Id.* Under the SCA, service providers may only be compelled to disclose a specific list of metadata or the contents of user's messages to law enforcement. *Id.*

circumstances—namely where law enforcement agents have legally obtained the user's username and password and are attempting to log in to his account from a new or unrecognizable device, without assistance from the user or ICP.[543] Even this protection varies, however, depending on how each ICP utilizes two-factor authentication.[544]

III. SECURITY PROGRAMS TAILORED TO ELIMINATING UNAUTHORIZED ACCESS TO USERS' ELECTRONIC COMMUNICATIONS

Preventing others—be they individual hackers or entire law enforcement agencies—from *entering* one's device or account is just one difficulty that users looking to secure their data must overcome.[545] Protecting the contents of communications sent through users' ICP accounts is the greater hurdle. The rise of ICPs that incorporate end-to-end encryption and ephemeral communications in their company practices have given users ironclad methods of protecting their data.[546] However, ICPs are directly governed by the SCA and must abide by its provisions.

A. *The Statutory Framework*

In 1986, before the rise of messaging apps and even the World Wide Web, Congress passed the ECPA to update federal wiretapping laws and to address privacy concerns in electronic communications.[547] The ECPA is divided into three separate and distinct sections.[548]

The first part of the ECPA features several amendments to the Wiretap Act.[549] The Wiretap Act describes the different types of authorized and unauthorized interceptions of wire, oral, and electronic communications.[550] Among other things, it authorizes providers of wire or electronic communications "to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral,

---

543. *See What Is Two-Factor Authentication and How Does It Work?*, *supra* note 81.

544. *Two-Step Verification*, *supra* note 85.

545. *See* Walt, *supra* note 5.

546. *See Id.*

547. *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197, 206 (2d Cir. 2016), *reh'g, en banc, denied*, 855 F.3d 53 (2d Cir. 2017).

548. CHARLES DOYLE, CONG. RESEARCH SERV., PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 1 (2012), https://www.hsdl.org/?view&did=725508.

549. *Electronic Communications Privacy Act (ECPA)*, EPIC.ORG, http://epic.org/privacy/ecpa/ (last visited Sept. 10, 2018).

550. 18 U.S.C. §§ 2510–2522.

or electronic communications or to conduct electronic surveillance, as defined in [S]ection 101 of the Foreign Intelligence Surveillance Act of 1978 . . . ."[551]

Title II of the ECPA is commonly referred to as the SCA.[552] The SCA reflects a congressional effort to create "Fourth Amendment-like privacy protections" applicable to electronic records and communications.[553] In other words, it was intended to assure users that their privacy expectations on the Internet would be promoted and their personal data kept safe.[554] Courts have held that users have a subjective expectation of privacy that society is prepared to deem reasonable in the contents of their email communications.[555] However, when dealing with communications sent via social media networks—ICP accounts among them—the determination of whether or not the SCA's protections extend to those communications depends on the particular actions of *the user*.[556] Usually, this involves an assessment of the privacy settings that the user has chosen to opt in on.[557] Users who limit the number or type of people who can see their Facebook "wall" postings are deemed to have taken steps to keep that information private; thus, courts have found that such postings, though they may be visible to some or many or even all of a user's Facebook friends, are protectable under the SCA because they are, "by definition, not accessible to the general public."[558]

In an attempt to provide strong privacy protections, the SCA divides service providers into two categories: electronic communications service ("ECS") and remote computing service ("RCS").[559] An ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[560] In contrast, an RCS is described as "the provision to the public of computer storage or

---

551. *Id.* § 2511(2)(a)(ii).

552. *In re Warrant Search Certain E-mail*, 829 F.3d at 205.

553. Christopher J. Borchert et al., *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36, 39 (2014–2015). The Fourth Amendment states that, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. CONST. amend. IV.

554. *See* 18 U.S.C. §§ 2701–2712 (2012); *Electronic Communications Privacy Act (ECPA)*, *supra* note 99.

555. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010). "Accordingly, we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'" *Id.*

556. Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 668 (D.N.J. 2013) (emphasis added). "Cases interpreting the SCA confirm that information is protectable as long as the communicator actively restricts the public from accessing the information." *Id.*

557. *Id.*

558. *Id.* "Privacy protection provided by the SCA does not depend on the number of Facebook friends that a user has." *Id.*

559. Borchert et al., *supra* note 30, at 103.

560. 18 U.S.C. § 2510(15).

processing services by means of an electronic communications system."[561] Both types of providers are generally prohibited from disclosing their users' communications, though there are several exceptions under which the providers may voluntarily disclose certain information.[562]

Due to the outdated distinction between ECS and RCS providers, the law has been unclear regarding the category that ICPs fall under.[563] Private messaging services offered by social media networks, such as MySpace and Facebook, affect the category that such providers fall under.[564] For example, some courts have held that these social networks operate as ECS providers when unopened private messages are at issue, but operate as RCS providers when the messages have been viewed and retained.[565] In the former scenario, the message is in "temporary, intermediate storage" awaiting review by the user.[566] In the latter scenario, the user has already opened and viewed the message, and made the conscious decision to retain it on the provider's network.[567] This decision reflects the user's preservation of the message "solely for the purpose of providing storage."[568] Regardless of the category that ICPs fall under, the security features they incorporate have the exact same effect on their inability to comply with compelled disclosure laws.[569]

Law enforcement agents may compel RCS and ECS providers to disclose two different types of data: (1) the contents of users' communications; and (2) specific non-content information, or metadata.[570] Metadata includes a user's name, address, telephone records or comparable records of session times and durations, length of services, types of services utilized, subscriber identity, and payment means for services.[571] Disclosure of metadata of this sort may be compelled from both ECS and RCS providers if an administrative subpoena "authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena" is obtained.[572] Notice to the user of this disclosure to law enforcement is not required.[573]

---

561. *Id.* § 2711(2).
562. *Id.* § 2702.
563. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989-90 (C.D. Cal. 2010).
564. *See id.*
565. *Id.*
566. 18 U.S.C. § 2510(17); *Crispin*, 717 F. Supp. 2d at 989.
567. *Crispin*, 717 F. Supp. 2d at 989.
568. 18 U.S.C. § 2703(b)(2)(B); *Crispin*, 717 F. Supp. 2d at 989.
569. *See infra* Part IV.
570. Borchert et al., *supra* note 30, at 103.
571. 18 U.S.C. § 2703(c)(2).
572. *Id.*
573. *Id.* § 2703(c)(3).

The requirements for compelled disclosure of the contents of communications are different depending on the type of service provider that is being compelled.[574] The contents of a user's communication may be compelled from an RCS provider, without notice to the user, if law enforcement agents obtain "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction."[575] If prior notice is given to the user, then the contents may be obtained in one of two ways.[576] The first option is for law enforcement to obtain an "administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena."[577] The second is for them to obtain a court order issued upon the production of "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[578]

To obtain the contents of a user's communications from an ECS provider, law enforcement has two alternatives.[579] If the communication is one hundred eighty days old or less, then the data may only be obtained pursuant to a warrant.[580] However, if the data is more than one hundred eighty days old, then the same procedures that apply to obtaining content from RCS providers apply.[581] Law enforcement may either choose to obtain a warrant without prior notice to the user, or they may notify the user and either obtain an administrative subpoena or a court order as previously described.[582]

Additionally, a request for backup preservation of the contents of a user's communications may be submitted by law enforcement.[583] Such a request must be accompanied by a subpoena or court order of the type previously mentioned.[584] This request would compel either service provider to "create a backup copy of the contents of the electronic communications sought in order to preserve those communications."[585] Notice to the user of the request or the subsequent compliance

---

574. Borchert et al., *supra* note 30, at 103.
575. 18 U.S.C. § 2703(b).
576. *Id.*
577. *Id.* § 2703(b)(B)(i).
578. *Id.* § 2703(b)(B)(ii), (d).
579. *Id.* § 2703(a).
580. 18 U.S.C. § 2703(a).
581. *Id.*
582. *Id.*
583. *Id.* § 2704.
584. *Id.* § 2704(a).
585. 18 U.S.C. § 2704(a).

with the request is not required.[586] While the SCA states that backup copies must be created within two days of the receipt of the request, it also notes that the service provider "shall create such backup copy as soon as practicable consistent with its regular business practices."[587]

The last section of the ECPA creates a chapter which addresses the use of pen registers and trap and trace devices.[588] While generally prohibiting the use of such devices, this section of the ECPA provides guidelines for using them in certain narrow exceptions.[589] Pen registers and trap and trace devices typically gather non-content data about users' communications.[590] This includes the phone numbers and email addresses of both incoming and outgoing messages, though no part of the content of the message is recorded.[591]

B. *End-to-End Encryption*

End-to-end encryption protects the contents of messages sent between two or more users.[592] End-to-end encryption entails the same scramble- and unscramble-process present in general encryption.[593] However, it operates in a slightly different manner that is uniquely tailored to safeguarding communications in transit.[594] End-to-end encryption software works by scrambling, or encrypting, a sender's message before it is transmitted to the receiver.[595] Thus, when the message leaves the sender's possession, it is already encrypted and cannot be viewed in an intelligible format by anyone intercepting the message—hackers, governments, and ICPs alike.[596] It is only decrypted once it is in the intended recipient's possession because only he has the key that can decrypt the message.[597] Essentially, this means that ICPs with end-to-end encryption have access to, and may store, the encrypted versions of its users' communications.[598] Such versions, however, are completely useless to them and to anyone that obtains them because no one but the rightful recipient has the code or key

---

586. *Id.*
587. *Id.*
588. *Id.* § 3121–3127.
589. *Id.* § 3121.
590. *Electronic Communications Privacy Act (ECPA)*, *supra* note 99.
591. *Id.* Thanks to portions of the USA Patriot Act, such devices may not record any part of the subject line of email communications because the subject line contains content. *Id.*
592. Unuth, *supra* note 40.
593. *Id.*
594. *Id.*
595. *Id.*
596. *Id.*
597. Unuth, *supra* note 40.
598. *See* Apuzzo, *supra* note 1.

to decrypt the message.[599] Thus, when an ICPs with this security feature is compelled to disclose the content of its users' messages to law enforcement, all it is capable of turning over is meaningless data.[600] This is the heart of the Going Dark Problem: government authorities are kept in the dark about the communications' contents despite having complied with the applicable legal process.[601]

This end result has become the pillar of many ICPs' reputations and an integral part of their privacy policies.[602] With end-to-end encryption systems in place, an ICPs' ability to comply with compelled disclosure laws has changed dramatically.[603] Many ICPs' privacy policies, data request policies, and legal guidelines reflect this change.[604] Apple's iMessage and FaceTime programs operate under this system, making it impossible for Apple to intercept its users' communications or decrypt the contents of their messages.[605] Similarly, Signal and WhatsApp operate under the same encryption software because it was designed by the same company—Open Whisper Systems.[606] In explaining end-to-end encryption, WhatsApp has echoed the core values of its company: "Privacy and security is in our DNA, which is why we have end-to-end encryption in the latest versions of our app."[607] Its law enforcement guidelines, while detailing its obligations under the SCA, clearly note that the encryption software it provides "means that messages are encrypted to protect against us and third parties from reading them."[608] In the same vein, Signal's privacy policy states that, "We cannot decrypt or otherwise access the content of a call or message."[609] Meanwhile, Slack provides "data encryption in transit and at rest" though the company does not

---

599. *See id.*

600. *Id.*

601. *Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, *supra* note 12.

602. Walt, *supra* note 5.

603. Apuzzo, *supra* note 1; Lance Whitney, *WhatsApp Faces Standoff with Feds over Its Message Encryption*, CNET (Mar. 14, 2016, 7:52 AM), http://www.cnet.com/news/whatsapp-faces-standoff-with-feds-over-its-message-encryption/.

604. *See, e.g.*, *Legal Process Guidelines*, *supra* note 22.

605. *Id.* "iMessage communications are end-to-end encrypted and Apple has no way to decrypt iMessage data when it is in transit between devices. Apple cannot intercept iMessage communications . . . ." *Id.*

606. Russell Brandom, *Feds Secretly Subpoenaed the Encrypted Chat App Signal Earlier This Year*, VERGE (Oct. 4, 2016, 10:30 AM), http://www.theverge.com/2016/10/4/13161026/signal-subpoena-court-order-encryption-police-open-whisper.

607. *End-to-End Encryption*, *supra* note 6. "WhatsApp's end-to-end encryption ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even WhatsApp." *Id.*

608. *Information for Law Enforcement Authorities*, WHATSAPP, https://www.whatsapp.com/legal/Information-for-Law-Enforcement-Authorities-(EN).pdf (last visited Sept. 10, 2018).

609. *Privacy Policy*, OPEN WHISPER SYSTEMS, http://signal.org/legal/ (last visited Sept. 10, 2018).

specify whether this entails the use of end-to-end encryption or another variation of encryption.[610]

To be clear, end-to-end encryption makes it impossible for ICPs to disclose only the contents of users' messages.[611] Various types of metadata and logs may still be retained and disclosed, depending on the company's regular business practices.[612] For certain ICPs, like Signal, it is routine practice to keep no user logs, whatsoever; therefore, subpoenas for those records come up just as empty as subpoenas for the contents of users' communications.[613]

Telegram's commitment to data security and privacy is particularly fascinating given its founder's background.[614] Pavel Durov designed Telegram in an effort to protect communications with his brother from interception and surveillance by the Russian government.[615] It, therefore, made perfect sense that Durov incorporated end-to-end encryption in his creation.[616] Telegram offers two modes of communication—Cloud Chats and Secret Chats.[617] Cloud Chats are heavily encrypted and stored on the company's servers so that users may access their data history whenever they please.[618] Secret Chats, on the other hand, are end-to-end encrypted and never stored on Telegram's servers.[619] As a result, communications in Secret Chats do not furnish Telegram with any data to disclose to law enforcement.[620] Further, the ICP does not

---

610. *Security Practices*, *supra* note 6.

611. *See* Thomas Fox-Brewster, *Forget About Backdoors, This Is the Data WhatsApp Actually Hands to Cops*, FORBES (Jan. 22, 2017, 10:00 AM), https://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/#20262ffa1030.

612. *Id.* "[T]here's little indication WhatsApp has ever handed message content to the cops . . . . Mostly it's metadata showing which numbers contacted which over WhatsApp, when, and for how long, as well as the IP addresses and phone identifiers associated with the subpoenaed accounts." *Id.*

613. *Id.*

614. Walt, *supra* note 5.

615. *Id.* Durov founded Russia's first Facebook-like social network, VKontakte. *Id.* The $3-billion company is now Europe's largest social network. *Id.* Despite this wild success, Durov was eventually fired as CEO of the company and then left Russia after several clashes with Russian authorities. *Id.* On one occasion, armed law enforcement authorities twice swarmed his apartment and threatened to break in if he didn't delete a Russian opposition leader's VKontakte account. Walt, *supra* note 5. On another, he was ordered to disclose the personal data of several opposition leaders from their social media accounts. *Id.* Both times, he refused. *Id.* Following these experiences, he designed Telegram. *Id.*

616. *Id.*

617. *Privacy Policy*, TELEGRAM, http://telegram.org/privacy (last visited Sept. 10, 2018).

618. *Id.*

619. *Id.*

620. *Id.* "Secret chats use end-to-end encryption, thanks to which we don't have any data to disclose." *Do You Process Data Requests?*, TELEGRAM: FAQ, http://telegram.org/faq#q-do-you-process-data-requests (last visited Sept. 10, 2018).

keep logs of communications sent via Secret Chats.[621] Media files sent in these chats are also end-to-end encrypted, but the encrypted versions of the files are stored on Telegram's servers; this stored data is periodically purged from the servers.[622]

To demonstrate the ironclad security provided by its end-to-end encryption, Telegram has hosted several contests challenging users to hack pieces of encrypted data.[623] One contest challenged users to decipher intercepted messages.[624] Another one directed participants to extract an email address from a Secret Chat between two users.[625] If a chance to publicly humiliate a popular company weren't enough to motivate users to participate, there was also the $300,000 cash prize for anyone who cracked Telegram's encryption in the second contest.[626] And if that weren't enough, then there was also the bonus objective—featuring a similar encryption challenge—with its own independent cash prize of $100,000.[627] None of the contests have ever produced a winner.[628]

Not all of Telegram's encryption publicity has been positive, however.[629] Following the terrorist attacks in Paris in November of 2015, it was revealed that ISIS members had used Telegram to communicate with each other.[630] The end-to-end encryption in Telegram's Secret Chats afforded their communications protection from surveillance by government entities.[631] Despite this revelation, Telegram still stands by its commitment to data privacy and proudly proclaims that, "So far, [disclosure of user information] has never happened."[632]

Of course, part of the reason that Telegram has disclosed zero bytes of user data to the U.S. government is because the company is not governed by U.S. laws.[633] At least, not solely by U.S. laws.[634] Rather, it uses a *distributed infrastructure* that scatters its servers around the world, so that no one government or country can acquire meaningful possession of a user's cloud chat communications.[635] This is because the decryption keys and the data they're meant to protect are distributed among different

---

621. *Privacy Policy*, *supra* note 167.
622. *Id.*
623. *$300,000 for Cracking Telegram Encryption*, TELEGRAM (Nov. 4, 2014), http://telegram.org/blog/cryptocontest.
624. *Id.*
625. *Id.*
626. *Id.*
627. *Id.*
628. *$300,000 for Cracking Telegram Encryption*, *supra* note 173.
629. Walt, *supra* note 5.
630. *Id.*
631. *Id.*
632. *Privacy Policy*, *supra* note 167.
633. *Do You Process Data Requests?*, *supra* note 170.
634. *Id.*
635. *Id.*

geographic regions.[636] Thus, if someone were to gain access to the decryption key for a specific message, he would also have to acquire possession of the data itself, which is stored in an entirely different legal jurisdiction.[637] Without both pieces of the puzzle, government entities would never see the big picture—the content of the message.[638]

The success of this tactic, however, will likely suffer in the face of the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), which was enacted as part of the Consolidated Appropriations Act on March 23, 2018.[639] The CLOUD Act amended the SCA by adding a provision which requires ICPs to comply with any type of SCA request "regardless of whether such communication, record, or other information is located within or outside of the United States."[640] The extraterritorial location of ICPs' servers or stored information does not discharge their legal obligation to comply with proper preservation, disclosure, and back-up requests.[641] Microsoft Corp. learned this lesson the hard way when it challenged an 18 U.S.C. § 2703 disclosure request in court.[642] Federal agents served Microsoft with a warrant for the email contents of one of its users' accounts.[643] Microsoft moved to quash the warrant on the ground that the email contents were stored in its datacenter in Ireland.[644] By the time the case reached the Supreme Court of the United States, Congress had already enacted the CLOUD Act and the government had obtained a new warrant pursuant to the new provision.[645] Accordingly, the Supreme Court held that the issue was moot, leaving Microsoft to comply with the new warrant.[646]

Other companies have employed similar tactics regarding physical storage of servers and data.[647] Where they are not "U.S. providers," ICPs are not subject to the CLOUD Act.[648] For example, ProtonMail is an email service provider domiciled in and governed by the laws of Switzerland.[649] Its founders made the strategic decision to incorporate the company in a country known for its strong privacy protection

---

636. *Id.*
637. *Id.* "[S]everal court orders from different jurisdictions are required to force us to give up any data." *Do You Process Data Requests?*, *supra* note 170.
638. *Id.*
639. Consolidated Appropriations Act, H.R. 1625, 115th Cong. (2018).
640. Clarifying Lawful Overseas Use of Data Act, § 103(a)(1) (to be codified at 18 U.S.C. § 2713).
641. *Id.*
642. United States v. Microsoft Corp., 138 S. Ct. 1186, 1187 (2018).
643. *Id.*
644. *Id.*
645. *Id.* at 1187–88.
646. *Id.* at 1188.
647. *See Privacy Policy*, PROTONMAIL, http://protonmail.com/privacy-policy (last visited Sept. 10, 2018).
648. *See Microsoft Corp.*, 138 S. Ct. at 1187.
649. *Privacy Policy*, *supra* note 197.

laws.[650] Under Swiss federal laws, "[T]he obligation to provide the technical means for lawful interception is imposed only on Internet access providers so [ProtonMail], as an Internet application provider, is not subject to this obligation and cannot be compelled to build in the technical means to intercept customer communications."[651]

It is precisely this type of obligation that has facilitated legal conflicts and disputes in the U.S. between law enforcement agencies and ICPs operating with end-to-end encryption software.[652] In the past two years, law enforcement authorities have been feeling the chilling effect of this revolutionary technological development.[653] Specifically, government entities have realized that wiretap and compelled disclosure orders pursuant to various provisions of the SCA have lost every ounce of power they previously carried.[654] This is chiefly because the orders can be complied with, but will produce nothing more than the meaningless jargon characteristic of encrypted messages.[655] In 2016, a federal judge approved a wiretap order of a WhatsApp user's communications.[656] Although WhatsApp fully complied with the order, its end-to-end encryption software was said to stymie the government's ability to actually read the messages it intercepted.[657] With end-to-end encryption in place, neither WhatsApp nor the government could decode the contents of the communications.[658]

As a result, government entities have advocated a solution to the problem that would surge power back into compelled disclosure laws.[659] In a move that threatens the very identity of most ICPs, law enforcement has suggested that ICPs create decryption software that would enable them to obtain the plaintext contents of users' messages.[660] In other words, the government seeks to "commandeer private engineers

---

650. *Id.* ProtonMail's servers are further protected by their location. *Security Details*, PROTONMAIL, http://protonmail.com/security-details (last visited Sept. 10, 2018). "Our primary datacenter is located under [one thousand] meters of granite rock in a heavily guarded bunker which can survive a nuclear attack." *Id.*

651. *Privacy Policy*, *supra* note 197.

652. Apuzzo, *supra* note 1; Whitney, *supra* note 153.

653. Apuzzo, *supra* note 1.

654. *See id.*

655. *Id.*

656. Whitney, *supra* note 153.

657. Apuzzo, *supra* note 1. "In the last year, the company has been adding encryption to those conversations, making it impossible for the Justice Department to read or eavesdrop, even with a judge's wiretap order." *Id.*

658. Whitney, *supra* note 153. "But the messages are encrypted, meaning no one, not even WhatsApp, can unscramble them so that they're readable." *Id.*

659. *See* Whitney, *supra* note 153.

660. *Id.* "But [Ex-F.B.I. Director James B. Comey] has called for technology companies and the government to find a middle ground that allows for strong encryption but accommodates law enforcement efforts." Apuzzo, *supra* note 1. "The Justice Department is reportedly trying to decide if it should ask a judge to force WhatsApp to find a way to decode the messages." Whitney, *supra* note 153.

working for private companies to write computer code that would disable the security protections their employers have designed into their products."[661] However, the law may not support this extension of government power.[662]

Courts have held that source code qualifies as language and, by extension, as speech that is privy to the protections afforded by the First Amendment.[663] This finding alone, however, does not take ICPs out of the purview of the All Writs Act.[664] Pursuant to the Act, law enforcement agencies recently moved to compel the device manufacturer Apple to design software—by writing source code—that would undermine the encryption protections of users' iPhone passwords, allowing agents to unlock such devices when users fail to disclose their passwords.[665] Government agencies are already considering making a similar argument in regards to ICPs' end-to-end encryption of communications sent via its systems.[666] In other words, ICPs would be compelled to design and create software for the sole purpose of enabling law enforcement agents to decode users' messages.[667] In Apple's case, *amici* pointed out the limitations of the All Writs Act and the inability of the government to use it as a means of forcing companies to redesign their products altogether.[668] In fact, they emphasized the fact that the way companies store their users' data is much more than a mere marketing strategy; above all else, "It is at the core of the products' identities."[669] In "conscript[ing] companies into defeating their own security safeguards and product designs," the government is exceeding the residual source of authority that the All Writs Act was intended to provide.[670]

Rather than using the All Writs Act to override the security features apps have deliberately included in their products, government agencies should turn to the identical approach taken by CALEA and the Swiss federal laws.[671] Both statutes prohibit government entities from compelling specific service providers to design or

---

661. Brief for Amazon.com et al. as Amici Curiae Supporting Apple, Inc. at 15, *In re* the Search of an Apple Iphone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 16-10 (C.D. Cal. Feb. 16, 2016).

662. *Id.*

663. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 449-50 (2d Cir. 2001); Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996), *superseded by* 974 F. Supp. 1288 (N.D. Cal. 1997).

664. Brief for Amazon.com et al. as Amici Curiae Supporting Apple, Inc., *supra* note 211, at 15.

665. *See id.* at 16.

666. Whitney, *supra* note 153.

667. *Id.*

668. Brief for Amazon.com et al. as Amici Curiae Supporting Apple, Inc., *supra* note 211, at 15.

669. *Id.* at 17.

670. *Id.* at 15.

671. *See* 47 U.S.C. § 1002(b); *Privacy Policy*, *supra* note 197.

adopt the technical means for lawful government interception of users' communications.[672] While Swiss law applies these compulsion protections to internet application providers of the sort discussed in this Comment, it does not do so for internet access providers.[673] In contrast, CALEA exempts ICPs from its provisions, meaning that the protection against compelled technical assistance solely extends to telecommunications providers.[674] If the SCA were amended to include a similar provision that applied to ICPs, the government would act in accordance with the privacy expectations of users that are evident in the various security features that companies have incorporated in recent years.[675]

C. *Ephemeral Communications*

The concept is simple: never leave a trace.[676] Thanks to ephemeral communications, the execution is just as simple with this security feature, which is the closest thing users have to not leaving a digital trace of their communications.[677] Ephemeral communications, as the name suggests, are short-lived messages that are deleted on a schedule that either the ICP or the user sets in advance.[678] Many ICPs have message and file retention features that users can take advantage of.[679] Among them, Slack gives users the greatest flexibility in scheduling the deletion of their messages.[680] Team administrators can opt to delete the contents of messages sent on either a team-wide or per-channel basis.[681] The shortest setting available is one day, so messages and files are automatically deleted by the Slack after every twenty-four-

---

672. 47 U.S.C. § 1002(b); *Privacy Policy*, *supra* note 197.

673. *Privacy Policy*, *supra* note 197. Thus, internet access providers may be compelled to provide the technical means for the Swiss government to intercept users' communications, but internet application providers may not be compelled to do so. *Id.*

674. 47 U.S.C. § 1002.

675. *See* Walt, *supra* note 5. "And for global companies, encryption has become a key strategy for growth, with customers far more focused on how to protect their private data, and as governments debate the issue." *Id.*

676. *See When Does Snapchat Delete Snaps and Chats?*, SNAPCHAT: SUPPORT, http://support.snapchat.com/en-US/a/when-are-snaps-chats-deleted (last visited Sept. 10, 2018).

677. *See id.*

678. *See Customize Message and File Retention Policies*, SLACK, http://get.slack.help/hc/en-us/articles/203457187-Custom-message-and-file-retention (last visited Sept. 10, 2018).

679. *See id.*

680. *Id.*

681. *Id.*

hour period.[682] Slack warns that messages which are deleted in this manner are *irretrievable*.[683]

Snapchat's reputation for privacy is rooted in ephemeral communications, as the application is almost entirely designed around this one safeguard.[684] It prides itself on having this signature feature, touting that *delete is our default*.[685] Once a snap or chat has been viewed by the user it was sent to, the message is permanently deleted from the sender's account, the recipient's account, and Snapchat's servers.[686] The company's law enforcement guidelines even reflect this practice, stating that it may only disclose the contents of users' communications in a very narrow set of circumstances, i.e. when the message has not otherwise been deleted.[687] Snapchat's deletion policy does not apply to snaps that have been saved in a user's Memories archive or that have not been opened.[688] However, even unopened snaps are eventually deleted, though that is done thirty days after the snap was sent.[689] Story content is, at the most, available for twenty-four hours provided that the user does not delete the content before then.[690] Additionally, the feature provides no protection against users who take screenshots of the messages prior to them being deleted.[691]

WhatsApp gives users the best of both worlds by combining the two strongest security features in its system.[692] Not only does the app end-to-end encrypt its users' messages, but it also incorporates ephemeral communications since "WhatsApp does not store messages once they are delivered or transaction logs of such delivered messages."[693] Like Snapchat, undelivered messages are deleted from WhatsApp's servers after thirty days.[694] Telegram also incorporates ephemeral communications though they are referred to as *self-destructing messages*.[695] In essence, the concept is the same but the user does not have the option of setting a file retention schedule.[696]

---

682. *Id.*

683. *Customize Message and File Retention Policies*, *supra* note 228. "Within [twenty-four] hours of workspace Primary Owner initiated deletion, Slack hard deletes all information from currently-running production systems . . . ." *Security Practices*, *supra* note 6. "Slack services backups are destroyed within [fourteen] days." *Id.*

684. *See When Does Snapchat Delete Snaps and Chats?*, *supra* note 226.

685. *Id.*

686. SNAPCHAT, INC., LAW ENFORCEMENT GUIDE 9 (2018), http://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf.

687. *Id.*

688. *Id.*

689. *Id.*

690. *Id.*

691. *When Does Snapchat Delete Snaps and Chats?*, *supra* note 226.

692. *See Information for Law Enforcement Authorities*, *supra* note 158.

693. *Id.*

694. *Id.*

695. *Privacy Policy*, *supra* note 167.

696. *Id.*

Rather, communications sent through Secret Chats automatically self-destruct once they have been viewed if the user has opted in to this feature.[697]

Just as with end-to-end encryption, ICPs that feature ephemeral communications hinder law enforcement's ability to obtain the contents of users' communications, even with a valid search warrant issued pursuant to the SCA.[698] With no copy of the messages on its servers, ICPs with this feature have nothing to disclose to law enforcement despite being legally compelled to do so.[699] Therefore, much of the same analysis that applies to end-to-end encryption also applies to ephemeral communications.[700] The development and wide popularity of this feature reflect an expectation of privacy on the part of users when it comes to communications sent via apps that incorporate ephemeral messaging.[701] The SCA should be amended to mirror the privacy expectations of ICPs' users.[702] In particular, this would mean that ICPs should not be prohibited by government entities from incorporating this security feature into their systems.[703] If apps can't be forced to create source code, then they definitely shouldn't be forced to refrain from using code that's already been created.[704]

IV. LIKELY OUTCOMES AND VIABLE SOLUTIONS TO THE GOING DARK PROBLEM

The statutory framework—the ECPA and SCA, in particular—is designed to provide the proper balance among several competing interests.[705] The driving force behind the statutes is the protection of Americans' privacy rights in communications sent using a novel medium—the Internet.[706] But individual privacy rights of this kind inevitably implicate legitimate law enforcement needs in public safety and national security.[707] Against this backdrop, the public and the law have brought to light the significance of a third interest—"encouraging the use and development of new

---

697. *Id.* "As soon as such a message is read ([two] checks appear), the countdown starts. When the timer expires, both devices participating in a secret chat are instructed to delete the message (photo, video, etc.)." *Id.*

698. *See* SNAPCHAT, INC., *supra* note 236, at 9.

699. *Id.*

700. *See supra* Part IV, Section A.

701. *See* Walt, *supra* note 5.

702. *See id.*

703. *See* 47 U.S.C. § 1002(b)(1).

704. *See id.*

705. *See Facebook, Inc. v. Superior Court*, 417 P. 3d 725, 737 (2018).

706. *Crispin*, 717 F. Supp. 2d at 971.

707. *In re Order Requiring Apple to Assist*, 2015 WL 5920207, at *1–2; *Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, supra note 12.

technologies."[708] As the catalyst for the law in the first place, this third interest rightly deserves its own consideration.[709]

This balancing act—between the public and private interests that are implicated—has repeatedly been placed in the hands of the judiciary.[710] But time and again, courts have properly attempted to shift the burden back where it belongs—in the hands of elected officials.[711] Judges have become powerful advocates, reflecting the widespread push for legislative reform of the existing statutory framework.[712] As the Ninth Circuit aptly noted in *Konop v. Hawaiian Airlines, Inc.*,[713] "until Congress brings the laws in line with modern technology, protection of the Internet . . . will remain a confusing and uncertain area of the law."[714]

Proposed bills and draft legislation introduced from both sides have fallen far short of serious congressional consideration.[715] Senate hearings featuring testimony about the Going Dark Problem from former Deputy Attorney General Sally Yates and former FBI Director James B. Comey have shown equal promise.[716]

No compulsory duty currently exists for ICPs to provide law enforcement with the technical assistance necessary to access users' communications.[717] But the existence of this exact duty on other types of providers suggests that this could be the direction Congress heads in when—*if*—it chooses to address the statutory gap.[718] In creating this duty, Congress will likely borrow language from sister statutes that apply the same requirement to other types of communications providers.[719] The Wiretap Act directs providers of wire and electronic communication services to "furnish [law

---

[708]. *Facebook, Inc. v. Superior Court*, 417 P. 3d 725, 737 (2018).

[709]. *See id.*

[710]. *Ehling*, 961 F. Supp. 2d at 666 (stating that, "the 'task of adapting the [SCA's] language to modern technology has fallen largely upon the courts.'") (quoting *United States v. Riggs*, 739 F. Supp. 414, 417 n.4 (N.D. Ill. 1990).

[711]. *Universal City Studios, Inc. v. Corley*, 273 F. 3d 429, 458 (2d Cir. 2001); *Ehling*, 961 F. Supp. 2d at 666 n.2; *Crispin*, 717 F. Supp. 2d at 988.

[712]. *Ehling*, 961 F. Supp. 2d at 666. In the words of United States District Court Judge William J. Martini, "Most courts, including this one, would prefer that Congress update the [SCA] to take into account the invention of the Internet." *Id.*

[713]. 302 F. 3d 868 (9th Cir. 2002).

[714]. *Id.* at 874.

[715]. ECPA Modernization Act of 2017, S. 1657, 115th Cong. (2017); Grid Cybersecurity Research and Development Act, H.R. 4120, 115th Cong. (2017); Secure Data Act of 2015, S. 135, 114th Cong. (2015); Secure Data Act of 2015, H.R. 726, 114th Cong. (2015); End Warrantless Surveillance of Americans Act, H.R. 2233, 114th Cong. (2015).

[716]. *Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, *supra* note 12.

[717]. *In re Order Requiring Apple, Inc. to Assist*, 2015 WL 5920207, at *1–2.

[718]. *See, e.g.*, Wiretap Act, 18 U.S.C. § 2518 (2018).

[719]. *See* 18 U.S.C. § 2518; Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1805(c)(2)(B) (2018).

enforcement] forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively."[720] An identical duty with nearly identical language is imposed under the Foreign Intelligence Surveillance Act of 1978 ("FISA"), though it applies to electronic surveillance of wire or radio communications.[721] A proposed Senate bill currently under consideration by the 115th Congress is quite instructive on this point.[722] This is because the bill is actually intended to modernize and amend the ECPA and SCA.[723] One provision in particular requires providers—ICPs included—to furnish law enforcement with "all information, facilities, and technical assistance necessary to accomplish the acquisition" of a user's geolocation information.[724] While the bill uses the language of the ECPA's sister statutes and expands the scope of the ECPA to geolocation information, it fails to address any of the "going dark" concerns emphasized by judges, law enforcement agencies, and privacy advocates alike.[725] This may explain the lack of legislative action on the bill since it was first introduced in the Senate on July 27, 2017.[726]

By far, however, CALEA contains the most thorough framework for the imposition of this duty.[727] CALEA applies to telecommunications carriers and does not extend to ICPs.[728] Telecommunications carriers must ensure that their equipment, facilities, or services can: (1) isolate and enable law enforcement to intercept all wire and electronic communications; (2) isolate and enable law enforcement to access call-identifying information; and (3) deliver the information in (1) and (2) to law enforcement.[729] To this extent, CALEA essentially mirrors the duty imposed under FISA and the Wiretap Act.[730] It differs from them, however, in two important respects.[731]

First, CALEA directly addresses encryption.[732] Under CALEA, carriers generally *do not* have a duty to decrypt communications or ensure the government's

---

720. 18 U.S.C. § 2518.

721. 50 U.S.C. § 1801(f)(1), 1805(c)(2)(B) (stating that providers shall "furnish [law enforcement] forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance").

722. ECPA Modernization Act of 2017, S. 1657, 115th Cong. (2017).

723. *Id.*

724. S. 1657 § 5.

725. *See id.*; 18 U.S.C. § 2518; 50 U.S.C. § 1805(c)(2)(B).

726. *See* S. 1657.

727. *See* 47 U.S.C. § 1002.

728. *In re Order Requiring Apple, Inc. to Assist*, 2015 WL 5920207, at *2 (stating that CALEA does not apply to "electronic mail, instant messaging, peer-to-peer communications, or social media.").

729. 47 U.S.C. § 1002.

730. *See id.*; 50 U.S.C. § 1805(c)(2)(B); 18 U.S.C. § 2518.

731. *See* 47 U.S.C. § 1002(b)(1), (3).

732. 47 U.S.C. § 1002(b)(3).

ability to decrypt them.[733] The only exception is when the carrier: (1) provides the encryption and (2) possesses the information needed to decrypt the communication.[734] If this provision is expanded by Congress to apply to ICPs, the latter prong would be susceptible to two varying interpretations.[735] On the one hand, the information needed to decrypt the communication may be referring to the source code, since that is the "key" to converting a message back to its original, intelligible form.[736] Since ICPs don't have the source codes—even when they provide the encryption service for the user—this reading gives them considerable leeway.[737] If they don't have the source code, they have no statutory duty to decrypt the communication or to help law enforcement decrypt it.[738] On the other hand, the language may be interpreted to refer to the encrypted content, itself.[739] If law enforcement can obtain the source code through other means, then the only other thing they need to successfully decrypt the communication is the encrypted version possessed by the ICP.[740] If this latter interpretation is adopted, then the statute affords some ICPs no protection because they are compelled to disclose what they *do* have—the scrambled communications.[741] This analysis only applies to ICPs that end-to-end encrypt their users' communications and back them up in some manner.[742] ICPs that employ ephemeral communications enjoy broader protection under this statutory framework because—without any stored version of the communication—they have nothing but metadata to disclose to law enforcement.[743]

Even more significantly, CALEA differs from its sister statutes by explicitly prohibiting law enforcement from commandeering ICPs.[744] Section 1002(b)(1) provides that the government is not authorized to require or prohibit the adoption of "any specific design of equipment, facilities, services, features, or system configurations . . . by any provider."[745] With this language alone, CALEA stands in stark contrast to the Wiretap Act and FISA.[746] If applied to ICPs, it ensures that the legal battle waged by the government against Apple in response to the San Bernardino

---

733. *Id.* (emphasis added).
734. *Id.*
735. *See id.*; Unuth, *supra* note 40.
736. Unuth, *supra* note 40.
737. Apuzzo, *supra* note 1.
738. *See* 47 U.S.C. § 1002(b)(3).
739. *See id.*
740. *See* Unuth, *supra* note 40.
741. *See* Apuzzo, *supra* note 1.
742. *See Information for Law Enforcement Authorities*, *supra* note 158.
743. *See* SNAPCHAT, INC., *supra* note 236, at 9.
744. *Brief for Amazon.com et al as Amici Curiae Supporting Apple, Inc.*, *supra* note 211, at 4; *see also* 47 U.S.C. § 1002(b)(1).
745. § 1002(b)(1).
746. *See* 47 U.S.C. § 1002(b)(1); 50 U.S.C. § 1805(c)(2)(B); 18 U.S.C. § 2518.

shooting will not be reincarnated against ICPs; the government could never use the judiciary to force ICPs to create a backdoor to their own security features.[747] This is particularly important given the cat-and-mouse game between law enforcement and technology-driven ICPs.[748] Because the adoption of the language in these two provisions—sections 1002(b)(1) and (3)—would categorically tip the balance in favor of ICPs, it is highly improbable that Congress will amend the SCA to include it.[749] This language would give ICPs even greater protection than they already enjoy and would do nothing to solve the Going Dark Problem.[750] On the contrary, it would only exacerbate it and make ICPs virtually untouchable by law enforcement.[751]

The best solution to the Going Dark Problem begins with taking the middleman out of the equation altogether.[752] Compelled disclosure laws—and compelled technical assistance provisions, in particular—fail to provide a sustainable solution that endures in the face of evolving technology.[753] With compelled disclosure laws, ICPs are forced to disclose information they simply do not have.[754] With compelled technical assistance provisions, ICPs are forced to build backdoors into their own products, thereby circumventing the very technologies they worked so hard to create.[755] Not to mention that these statutory requirements place ICPs in the impossible position of reconciling their mission statements with their statutory

---

[747]. *See Brief for Amazon.com et al as Amici Curiae Supporting Apple, Inc.*, *supra* note 211, at 4; Jack Nicas, *Apple to Close iPhone Security Hole That Law Enforcement Uses to Crack Devices*, N.Y. Times (June 13, 2018), http://www.nytimes.com/2018/06/13/technology/apple-iphone-police.html.

[748]. *See* Nicas, *supra* note 297. The use of encryption on Apple and Google smartphones prompted law enforcement to use every possible passcode combination to unlock phones. *Id.* Apple responded by creating software which automatically disabled a phone after a certain number of incorrect attempts. *Id.* The government countered by using third-party software which disabled that feature. *Id.* In response, Apple recently announced that it will be creating a software update which disables a phone's charging and data port an hour after the phone is locked—thereby preventing the government from circumventing its security features. *Id.*

[749]. *See* § 1002(b)(1), (3).

[750]. *See id.*; *Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, *supra* note 12.

[751]. *See* § 1002(b)(1), (3); *Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, *supra* note 12.

[752]. *See Whatsapp Privacy Policy*, *supra* note 7 ("End-to-end encryption means that your messages are encrypted *to protect against us and third parties* from reading them.") (emphasis added); *Privacy Policy*, *supra* note 167 ("We store messages, photos, videos and documents from your "cloud chats" on our servers so that you can access your data from any of your devices anytime *without having to rely on third-party backups*.") (emphasis added).

[753]. *Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, *supra* note 12.

[754]. *Id.*; *see also* 18 U.S.C. § 2703.

[755]. *Brief for Amazon.com et al as Amici Curiae Supporting Apple, Inc.*, *supra* note 211, at 18–20; *see also* 47 U.S.C. § 1002(b)(1).

duties.[756] User privacy is often the bedrock of an ICP's corporate identity, yet an ICP is forced to reveal its users' communications, or worse, work with law enforcement to override security programs and features it created to keep third parties like them, out.[757] As mere messengers, ICPs should not be punished for doing precisely what they were designed to do using the emerging technologies that its users demand and have come to expect.[758]

With that said, law enforcement does have alternate, viable solutions to the Going Dark Problem—two of which will benefit both the government and the public in the long-term.[759] For one, the government can better develop its own use of technology.[760] The Going Dark Problem originated with the advent of widespread encryption use in 2014.[761] In response, law enforcement agencies turned to often-undisclosed third parties for help.[762] Early on, such assistance came at a steep price—

---

[756]. *Compare Privacy Policy*, APPLE, http://www.apple.com/legal/privacy/en-ww/ (last updated May 22, 2018), *with* 18 U.S.C. § 2703, *and* 47 U.S.C. § 1002(b)(1).

[757]. *See Privacy Policy*, *supra* 306 ("Apple takes the security of your personal information very seriously."); *Security Practices*, *supra* note 6 ("We take the security of your data very seriously at Slack. As transparency is one of the principles on which our company is built, we aim to be as clear and open as we can about the way we handle security."); *WhatsApp Legal Info*, WhatsApp, http://www.whatsapp.com/legal/ (last visited Sept. 2, 2018) ("Respect for your privacy is coded into our DNA. Since we started WhatsApp, we've built our Services with a set of strong privacy principles in mind."); *Our Privacy Principles*, SNAP: PRIVACY CENTER, http://www.snap.com/en-US/privacy/privacy-center/ (last visited Sept. 10, 2018) ("At Snap, we make your privacy a priority."); SIGNAL, *supra* note 19 ("Privacy that fits in your pocket.").

[758]. *See Brief for Amazon.com et al as Amici Curiae Supporting Apple, Inc.*, *supra* note 211, at 18.

> Amici do not create security-protecting features just to satisfy their own ideological predilections. They also do so in response to "consumer demands to protect private data." . . . . As storing sensitive personal and commercial data electronically becomes less of a luxury and more of a necessity, protecting that data has also become a necessity.

Id. (citing Devlin Barrett et al., *Apple and Others Encrypt Phones, Fueling Government Standoff*, Wall St. J. (Nov. 18, 2014)).

[759]. *See* 18 U.S.C. § 2703(f); *Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, *supra* note 12, at 3–4.

[760]. *See Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, *supra* note 12, at 10 (stating, "[The Department of Justice] should also continue to invest in developing tools, techniques, and capabilities designed to mitigate the increasing technical challenges associated with the 'Going Dark' problem.").

[761]. Nicas, *supra* note 297; Craig Timberg & Tony Romm, *Apple is Making it Harder for Police to Collect Evidence from iPhones of Suspected Criminals*, WASH. POST (June 13, 2018), http://www.washingtonpost.com/news/the-switch/wp/2018/06/13/apple-is-making-it-harder-for-police-to-collect-evidence-from-iphones-of-suspected-criminals/?utm_term=.bca53f6cb545.

[762]. Nicas, *supra* note 297. Cellebrite and Grayshift are two companies which are known for providing law enforcement agencies with technical assistance in accessing information stored on locked iPhones. *Id.*

$1.3 million, to be exact.[763] But in keeping with basic principles of supply and demand, a greater demand for this type of assistance has led to a dip in prices.[764] In fact, law enforcement no longer needs third parties for technical assistance in accessing some forms of encrypted messages.[765] Efforts to access text messages stored on locked iPhones have been furthered by the creation of a device which law enforcement can simply purchase and use themselves.[766] This development presents a much more appealing solution to the Going Dark Problem.[767] Rather than relying on ICPs for technical assistance, the government should invest and hone in on the very technologies that created the Going Dark Problem in the first place.[768] This would prevent the need to outsource technical assistance to third parties and enable law enforcement to independently use and develop technologies.[769] Government agencies' improved use of, and greater access to, new and emerging technologies will advance public safety and national security without the involvement of ICPs.[770]

Another option for law enforcement is one that has been repeated time and time again—statutory amendment.[771] Instead of borrowing language from its sister statutes, however, the amendment should create an entirely new statutory process that accounts for the unique nature of the technologies used.[772] Ephemeral communications and end-to-end encryption are unique because communications are virtually inaccessible to anyone other than the intended recipients.[773] Currently, law enforcement can issue a preservation request requiring an ICP to "preserve a one-time data pull of the requested

---

763. *Id.*

764. *Id.* (stating that, "[l]aw enforcement officials said they generally send iPhones to Cellebrite to unlock, with each phone costing several thousand dollars to open.").

765. *Id.*

766. Nicas, *supra* note 297. New Apple software updates may thwart the use of this device. *Id.*

767. *See id.*

768. *See Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, *supra* note 12, at 1–3.

> American citizens care deeply about privacy and rightly so. Many companies have been responding to a market demand for products and services that protect the privacy and security of their customers. This has generated positive innovation that has been crucial to the digital economy. We, too, care about these important principles. Indeed, it is our obligation to uphold civil liberties, including the right to privacy.

Id. at 2.

769. *See* Nicas, *supra* note 297.

770. *See Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, *supra* note 12, at 10.

771. *Ehling*, 961 F. Supp. 2d at 666; Apuzzo, *supra* note 1.

772. *See Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, *supra* note 12, at 3.

773. Apuzzo, *supra* note 1; *When Does Snapchat Delete Snaps and Chats?*, *supra* note 226.

existing user data available at the time of the request for 90 days."[774] In other words, this type of preservation request applies to communications that have already been sent.[775] Legislators must create a process whereby a law enforcement agency can statutorily require an ICP to preserve the contents of a user's *future* communications for a short and specified period of time.[776] Any such request would, of course, have to be accompanied by proper judicial oversight in the form of a court order or search warrant.[777] This type of *prospective* approach gives ICPs a chance to comply with legitimate law enforcement needs without overriding their own security features. The success of this alternative, however, depends in large part on: (1) the technological ability to *disable*—rather than *bypass*—security features, and (2) law enforcement's ability to identify suspects and their respective accounts early on in investigations. The latter point can only be facilitated by the expenditure of substantial funds and resources, much like the first alternative noted above. The first point, meanwhile, shows great promise because some users already have the option of enabling or disabling end-to-end encryption.[778] For example, Telegram users can communicate either via Secret Chats—which use end-to-end encryption—or Cloud Chats—which, though heavily encrypted, do not.[779] The hurdle for ICPs is ensuring their own ability to disable security features such as these, independent of the user's selected preference.[780]

V. CONCLUSION

In recent years, ICPs have redefined their role in society.[781] By incorporating privacy policies, business practices, and security features that frustrate law enforcement's access to users' data, they have asserted their role as conduits of information.[782] They are mere messengers—carriers of their subscribers' data.[783] More importantly, however, they embody their users' market demands, and the way they do business is a direct manifestation of their users' privacy expectations in their

---

774. *Legal Process Guidelines*, *supra* note 22 (emphasis added); *see also* 18 U.S.C. § 2703(f) (stating that, upon request, an ECS or RCS must "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.").

775. *Legal Process Guidelines*, *supra* note 22.

776. *See* § 2511(2)(a)(ii) (authorizing providers of wire and electronic communication services to intercept communications and conduct surveillance).

777. § 2511(2)(a)(ii)(A)–(B).

778. *See Help Center: Secret Conversations*, FACEBOOK, http://www.facebook.com/help/messenger-app/1084673321594605/ (last visited Sept. 10, 2018).

779. *Privacy Policy*, *supra* note 167.

780. *See id.*

781. *See* Walt, *supra* note 5.

782. *See id.*; Apuzzo, *supra* note 1.

783. *See* Apuzzo, *supra* note 1; Walt, *supra* note 5.

Internet-based communications with others.[784] As the Department of Justice and Federal Bureau of Investigation openly concede, "we have on a new scale seen mainstream products and services designed in a way that gives *users* sole control over access to their data."[785] Rather than punishing ICPs by controlling—and effectively killing—the privacy features they incorporate in their applications, Congress should finally see these entities for what they really are—mere messengers.[786]

---

[784]. *See* Apuzzo, *supra* note 1; Walt, *supra* note 5.

[785]. *Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, *supra* note 12, at 3.

[786]. *See* Apuzzo, *supra* note 1; Walt, *supra* note 5; SIGNAL, *supra* note 19 ("Signal is made for you. As an Open Source project supported by grants and donations, Signal can *put users first.*") (emphasis added).