END-TO-END AUTHENTICATION: A FIRST AMENDMENT HOOK TO THE ENCRYPTION DEBATE

*LEONID GRINBERG**

* N.Y.U. School of Law, J.D., 2018; Massachusetts Institute of Technology, S.B., 2014; Editor-in-Chief, *Annual Survey of American Law*, 2017–18. The views expressed in this Note are solely mine and not my employer's. This Note was submitted in partial completion of the requirements of the Scholarship for Service, which has very generously supported my enrollment in law school. I would like to thank Zach Goldman and Randy Mitch for their leadership in the program during my time at NYU, and Zach Goldman in particular for his mentorship throughout this project. The *Annual Survey* has been my lifeline at NYU, and I would especially like to acknowledge the Notes Writing Program, Harry Black, and Brian Gottlieb for helping me develop this Note. I would also like to thank Ben Weissmann for insightful discussions in the early stages of this project. Finally, I would like to thank Beth Findley—for everything, really.

INTRODUCTION

The past few years have seen a proliferation of messaging services offering "end-to-end encryption."[1] The popularity of and demand for these services increased after Edward Snowden's 2013 leaks, which revealed that communication service providers were cooperating with state surveillance efforts.[2] A conversation that is encrypted "end to end" is one in which only the participants have access to the messages in a readable form. When messages are in transit, no one, including the service provider itself, has access to the unencrypted content. By encrypting messages from end to end, a messaging service provider can assure its users that cooperation with the government would be impossible because the company does not have the ability to decrypt the messages. Only when a message reaches its intended recipient can it be read intelligibly.[3]

One of the most prominent examples of end-to-end encrypted messaging services is Apple's iMessage,[4] which, as of 2016, processed 200,000 messages per second (which amounts to 63 quadrillion messages per year),[5] and has featured end-to-end encryption as a default setting since 2011.[6] There are plenty of other

1. Ken Kantzer, *Yet Another End-To-End Encrypted App*, PKC SECURITY (Dec. 16, 2016), https://www.pkcsecurity.com/yet-another.html [https://perma.cc/NGS4-7LAN] ("It seems that every week, yet another end-to-end encrypted app is unleashed on the world.").

2. *See generally* Mark Mazzetti & Michael S. Schmidt, *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance*, N.Y. TIMES (June 9, 2013), http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html. Media outlets across the world have posted the original leaked confidential, starting with Snowden's original trove. Much of this has been collected by the Electronic Frontier Foundation. *See NSA Primary Sources*, ELECTRONIC FRONTIER FOUND. https://www.eff.org/nsa-spying/nsadocs [https://perma.cc/J7PF-CXXJ].

3. Andy Greenberg, *Hacker Lexicon: What is End-to-End Encryption?*, WIRED (Nov. 25, 2014, 9:00 AM), https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/ [https://perma.cc/PV9Z-QEVB].

4. As of iOS 10, the iMessage app was renamed as "Messages," and "iMessage" became the name of a framework allowing third-party developers to add extension to the main app. *See iMessage Apps*, APPLE, https://developer.apple.com/imessage/ [https://perma.cc/LF37-NLWZ]. For simplicity and the distinctive name, this Note uses the name "iMessage" to describe the messaging service.

5. Kif Leswing, *Apple Says People Send as Many as 200,000 iMessages per Second*, BUS. INSIDER (Feb. 12, 2016, 2:08 PM), http://www.businessinsider.com/eddy-cue-200k-imessages-per-second-2016-2 [https://perma.cc/YA7P-QE93].

6. Press Release, Apple, New Version of iOS Includes Notification Center, iMessage, Newsstand, Twitter Integration Among 200 New Features (June 6, 2011), http://www.apple.com/pr/library/2011/06/06New-Version-of-iOS-Includes-Notification-Center-iMessage-Newsstand-Twitter-Integration-Among-200-New-Features.html [https://perma.cc/ZC8A-FSL6].

end-to-end encrypted messaging services available on the market, such as Facebook's WhatsApp, which boasts over one billion users of its own.[7] Facebook Messenger, which is built into the social networking website and is also available as a separate mobile application, also features end-to-end encryption, although it must be specially enabled by the user.[8] Consequently, a significant fraction of the world's population is communicating using end-to-end encryption, perhaps without even knowing it.[9]

Former FBI Director James Comey has referred to the proliferation in the use of end-to-end encrypted messaging services as the "going dark problem" and has argued that such services should be reined in.[10] Some commentators have breathed new life into a 1990s-era proposal called "key escrow," wherein the keys needed to decrypt a user's content would be preemptively given to the government but held "in escrow" until a valid court order grants access to

7. *One Billion*, WHATSAPP BLOG (Feb. 1, 2016), https://blog.whatsapp.com/616/One-billion [https://perma.cc/38N9-E98L].

8. *See* Gail Kent, *Hard Questions: Why Does Facebook Enable End-to-End Encryption*, FACEBOOK NEWSROOM (May 7, 2008), https://newsroom.fb.com/news/2018/05/end-to-end-encryption/ [https://perma.cc/WF6M-BPK2].

9. There is no single reason why the demand for end-to-end encryption is so high, even among the law-abiding. Some consumers distrust the government, either on principle or after news of some abuse. Reports about increased surveillance on mosques, for example, likely provided incentives for some Muslims to encrypt their communications to avoid harassment by the government. *Cf.* Lee Mathews, *Encrypted Email Signups Skyrocketed After Trump Victory*, FORBES (Nov. 14, 2016, 4:39 PM), https://www.forbes.com/sites/leemathews/2016/11/14/encrypted-email-signups-skyrocketed-after-trump-victory [https://perma.cc/7PKE-BPYK]. Others may be worrying not about the government but about hackers who could steal their personal or embarrassing communications from their service provider. In 2014, for example, a hacker accessed iCloud and Gmail accounts belonging to celebrities and posted nude photographs of them online. Tom Sykes, *Celebrity Nude Photo Hack: Images of Miley Cyrus, Kristen Stewart, Tiger Woods and More Leak Online*, THE DAILY BEAST (Aug. 22, 2017, 4:34 AM), https://www.thedailybeast.com/celebrity-nude-photo-hack-images-of-miley-cyrus-kristen-stewart-tiger-woods-and-more-leak-online [https://perma.cc/4FH9-TRY5]. Anyone who had stored only encrypted copies of the images would not have been affected by the hack.

10. *See, e.g.*, Adam Mazmanian, *Comey Renews Encryption Plea on Capitol Hill*, FCW (July 8, 2015), https://fcw.com/articles/2015/07/08/comey-encryption-hearing.aspx [https://perma.cc/6RX9-L5HN] ("The problem, as Comey sees it, is that criminals, terrorists and other malefactors are 'going dark,' by using end-to-end encryption built into mobile device operating systems offered by Apple and Google, and available in some communications software, like WhatsApp."); *see also Going Dark*, FBI, https://www.fbi.gov/services/operational-technology/going-dark [https://perma.cc/4BX6-JDAQ]; David E. Sanger & Sheera Frenkel, *"Five Eyes" Nations Quietly Demand Government Access to Encrypted Data*, N.Y. TIMES (Sept. 4, 2018), https://www.nytimes.com/2018/09/04/us/politics/government-access-encrypted-data.html [https://perma.cc/AGQ3-4MJT].

the key on a case-by-case basis.[11] Many civil rights and technical groups have responded negatively to this proposal[12] (just as they did two decades ago[13]). One of the most common critiques is that the government would be unable to adequately protect the billions of decryption keys it was holding "in escrow" against theft by criminals or rival state governments.[14]

The reality, however, is that key escrow would probably not be an effective method of solving the "going dark problem." Any two actors communicating on an uninterrupted, public connection can establish an encrypted channel of communication using simple, well-known algorithms, even in the presence of eavesdroppers.[15] Of course, the government could ban the creation of such software, but the simplicity and ubiquity of the code in computer science textbooks would undermine the ban.[16] Furthermore, history has shown that similar efforts have been unsuccessful. The Digital Millennium Copyright Act, for example, has done little to lessen the availability of file-sharing applications and websites, notwithstanding their illicit status.[17]

Therefore, the government will probably look for other ways to gain access to encrypted messages. In light of that, I propose focusing the discussion on *user authentication*—that is, technology that

11. *See, e.g.*, Ellen Nakashima & Barton Gellman, *As Encryption Spreads, U.S. Grapples with Clash Between Privacy, Security*, WASH. POST (Apr. 10, 2015), https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html [https://perma.cc/4L98-PNRH].

12. *E.g.*, HAROLD ABELSON ET AL., KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS, (2015), https://dspace.mit.edu/handle/1721.1/97690 [https://perma.cc/86QA-ATA4].

13. *E.g.*, HAL ABELSON ET AL., THE RISKS OF KEY RECOVERY, KEY ESCROW, AND TRUSTED THIRD-PARTY ENCRYPTION (1997), https://doi.org/10.7916/D8GM8F2W [https://perma.cc/Z2DU-2QMP].

14. *See, e.g.*, ABELSON ET AL., *supra* note 12, at 15 ("Providing access over any period of time to thousands of law enforcement agencies will necessarily increase the risk that intruders will hijack the exception access mechanisms. . . . . [T]he challenge of guaranteeing access to multiple law enforcement agencies in multiple countries is enormously complex. It is likely to be prohibitively expensive and also an intractable foreign affairs problem.").

15. *See* Greenberg, *supra* note 3. *See generally infra* Part I.

16. *See, e.g.*, Aaronson, *infra* note 100.

17. *See, e.g.*, Koren Helbig, *11 Numbers That Show How Prolific Illegal Downloading Is Right Now*, PRI (Apr. 20, 2014, 12:43 PM), https://www.pri.org/stories/2014-04-20/11-numbers-show-how-prolific-illegal-downloading-right-now [https://perma.cc/DPU9-93SY] (reporting that Americans illegally downloaded more than 96.8 million songs in 2012, more than any other country).

verifies for each user that the messages she reads come from the counterparty in the conversation—instead of focusing it on keys. As noted above and explained in detail below, any two individuals speaking on a reliable connection can establish an encrypted channel. Authentication is the technology that provides that reliability[18] through the use of keys that are known to be associated with a particular user. Thus, authentication is sufficient to establish an end-to-end encrypted conversation. But, though sufficient, it is also necessary. After all, for any conversation to remain confidential, each party must know *with whom* she is speaking. It does no good for the sender to encrypt a message for the recipient if the key used for the encryption actually belongs to a third party. End-to-end encryption could be effectively circumvented by any eavesdropper who could get his or her own key inserted into the users' encryption algorithms (a technique called a "man-in-the-middle attack"). If there were no reliable way for distributing keys and matching them to particular identities, this would be a very effective way for the government to listen in on encrypted conversations. The government could simply supply its own keys to a service provider and convince (or compel) it to claim that the keys are associated with a target user.

I am not aware of any case in which the government has actually replaced one user's keys with its own, but the possibility has been raised many times in the past, in both popular and technical literature.[19] In the case of iMessage, for example, even though Ap-

18. *See generally infra* Part I.B. By "reliability" I mean the abstract notion that messages are not tampered with or forged by others. The physical integrity of the channel—the audio quality of a phone conversation, for example—is assumed.

19. *See, e.g.*, Manisha Ganguly, *WhatsApp Design Feature Means Some Encrypted Messages Could Be Read by Third Party*, THE GUARDIAN (Jan. 13, 2017, 6:00 AM), https://www.theguardian.com/technology/2017/jan/13/whatsapp-design-feature-encrypted-messages [https://perma.cc/3H6K-HVDF] (describing the potential for the vulnerability in WhatsApp); *Apple's iMessage Defense Against Spying Has One Flaw*, WIRED (Sept. 8, 2015, 1:10 PM), https://www.wired.com/2015/09/apple-fighting-privacy-imessage-still-problems/ [https://perma.cc/L43K-KGZN]; Greenberg, *supra* note 3 ("Even end-to-end encryption isn't necessarily impervious from snooping. Rather than try to actually break the encryption, for instance, an eavesdropper may try to impersonate a message recipient so that messages are encrypted to their public key instead of the one the sender intended. After decrypting the message, the snoop can then encrypt it to the recipient's actual public key and send it on again to avoid detection."); Cyril Cattiaux et al., *iMessage Privacy*, QUARKSLAB (Oct. 17, 2013), http://blog.quarkslab.com/imessage-privacy.html [https://perma.cc/4W63-U3X5]; Matthew Green, *Can Apple read your iMessages?*, CRYPTOGRAPHY ENGINEERING (June 26, 2013), https://blog.cryptographyengineering.com/2013/06/26/can-apple-read-your-imessages/ [https://perma.cc/2PL3-BJJY].

ple never has access to unencrypted messages, nor the keys needed to decrypt encrypted messages, there is nothing stopping Apple from configuring its system to misreport the party with whom a user is speaking and encrypting a message so as to be readable by a third party. That third party could be the government.

It is not an accident that so much ink has been spilled on what seems like a hypothetical problem. The concern is not just about encryption. After all, authentication is useful for many applications, many having nothing to do with end-to-end encryption. Proving that one is who he or she claims to be is central to the Internet's functionality. Users would not be comfortable sending intimate emails or texts, or for that matter logging into a bank's website, if they were not confident that they were communicating with their lover or their bank. The government would be tampering with the technology that makes that confidence possible, which I am broadly referring to as "authentication" (and in the case of consumer messaging services, "user authentication").[20] And yet, as mentioned earlier, a reliable channel, with authenticated participants in the conversation, is sufficient on its own to create a confidential channel. In other words, unlike key escrow, which is widely resisted and is unlikely to work, this method is both very effective and has far-reaching consequences.

I refer to this hypothetical government technique as an "assisted man-in-the-middle (MITM) attack" and the corresponding hypothetical court order compelling assistance by the service provider as an "assisted MITM order." As mentioned above and explained further in Part I, a "man-in-the-middle attack" is a hacking technique in which an adversary intercepts communications and tampers with them in some way. In this context, the "adversary" (from the perspective of those wishing to keep their messages private) is the government and its "attack" is "assisted" by the service provider. As Part III emphasizes, the nuances of the roles the service provider and the government play are central to the discussion: the assistance from the service provider is not simply technical, but also communicative—it facilitates the process by placing its imprimatur on the communications provided by the government, making the communications seem as if they are coming from the service provider itself.

As cited earlier, there is plenty of prior technical work acknowledging the concerns about an assisted MITM attack. This paper explores the issue through a legal lens. Though very effective, an

20. *See generally infra* Part I.B.

assisted MITM attack is likely to have constitutional ramifications. An assisted MITM order implicates the compelled speech doctrine because it would require service providers to display and send particular messages chosen by the government, thus potentially violating the service providers' First Amendment rights. And because key distribution affects not just encryption but also authentication, there is a broader public policy concern—one that has less to do with conventional notions of privacy and more with identity. In an era in which an increasingly large percentage of communications take place over a network, anyone texting, emailing, or posting on social media has a higher stake in being able to digitally prove who they are to their audiences. The law has not yet evolved to recognize this need. Indeed, as this paper argues, assuming the Fourth Amendment is satisfied, *users'* constitutional rights are unlikely to be violated if the government acted in this way—even in circumstances where the users seemingly have strong free speech interests. This cutting-edge context raises novel questions as to whether the First Amendment *should* be extended to recognize such rights—a "right to integrity of identity," if you will—which heretofore have mostly been protected only, if at all, by common law and statutory personality rights.[21]

This Note proceeds in four Parts. Part I is a technical primer on encryption and authentication technologies. It explains in basic terms how the technologies work, describes iMessage (as an operative example) in some detail, and explains how the hypothetical surveillance technique would operate. It also briefly explains the relationship between the technologies and issues discussed in this Note and those in the controversy between Apple and the FBI following the San Bernardino terrorist attacks in 2015. Part II argues that there is existing statutory authority for the government to issue an assisted MITM order under the All Writs Act and the Stored Communications Act. It also highlights some legislation introduced after the Apple-FBI controversy. Part III argues that irrespective of the source of authority, the order would violate service providers' First Amendment rights. Part IV shifts the focus to the users and analyzes their interests. It concludes that absent a claim of injury by the service provider, such techniques would likely be constitutional and without remedy to the users. It suggests, however, that it may be worth considering an expansion of privacy rights in some in-

21. *See, e.g.*, Toney v. L'Oreal USA, Inc., 406 F.3d 905, 908–09 (7th Cir. 2005) (contrasting federal copyright in a given image with a state statute providing for a right of publicity, defined as "the very identity or persona of the plaintiff as a human being").

stances into a constitutional realm—motivated by the First, rather than the Fourth Amendment.

I.
A TECHNICAL PRIMER[22]

The issues discussed in this Note do not require any technical knowledge beyond familiarity with some common cryptographic concepts and terminology. This primer supplies that background.

A. Encryption

A fundamental building block of most cryptographic operations is the "*key*." A key is just a number, typically a very big one,[23] that is used as an input into some cryptographic process. In the case of "*encryption*," the key is used to "scramble" the message. "*Decryption*," the reverse operation, uses a key to "unscramble" the message. There are many different ways to implement an encryption scheme, some of which use the same key for both the encryption and decryption steps (this is called "*symmetric encryption*") and some of which use different but mathematically related keys ("*asymmetric encryption*").

Although end-to-end encryption in messaging services requires asymmetric encryption (the reason for that will be evident in a moment), basic symmetric encryption is a useful starting place for understanding encryption technology more generally. Thus, as a first, concrete example, consider a simple cipher in which the sender shifts the letters in her message by a predetermined amount. For

22. Because cryptography is such a vast subject whose technical details would not be of interest to most readers, I have chosen not to individually cite many of the general claims made in this primer. Instead, I direct interested readers to an excellent textbook by Professor Michael Sipser. *See generally* MICHAEL SIPSER, INTRODUCTION TO THE THEORY OF COMPUTATION ch. 10.6 (3d ed. 2013).

23. For example, the popular Advanced Encryption Standard, issued in 2001 by the National Institute of Standards and Technology, uses keys of at least 128 bits. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, ANNOUNCING THE ADVANCED ENCRYPTION STANDARD (AES) (2001), https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf [https://perma.cc/FD3Z-FEAT]. A key length of 128 bits translates to approximately 39 digits. One of the encryption keys used in iMessage (there are several layers of encryption involved) is 1280 bits, APPLE, IOS SECURITY 60 (2018), https://www.apple.com/business/docs/iOS_Security_Guide.pdf [https://perma.cc/JQ39-9GS7], which translates to approximately 887 digits. For comparison, the number of atoms in the observable universe has approximately 80 digits. John Carl Villanueva, *How Many Atoms Are There in the Universe?*, UNIVERSE TODAY (July 30, 2009), https://www.universetoday.com/36302/atoms-in-the-universe/ [https://perma.cc/RUL5-J7YF].

example, suppose the message is "HELLO" and the letters are to be shifted by a distance of 5. The resulting message is "MJQQT" (because "H" is the eighth letter in the alphabet and "M" is the thirteenth, "E" is the fifth letter and "J" is the tenth, and so on). The original "HELLO" message is called the "*plaintext*" whereas the incomprehensible "MJQQT" message is called the "*ciphertext*." The key used in this operation is "5"—the amount by which the letters were shifted. The shifting operation is the "encryption" step. After the recipient receives the ciphertext, he can shift the letters back down (the "decryption" step) by the key to recover the plaintext. The complete sequence of steps—the sender and recipient agree on a key, the sender shifts up every letter in the plaintext by the key to create the ciphertext, the sender transmits the ciphertext, the recipient shifts down every letter in the ciphertext by the same key to recover the plaintext—is called an "*encryption scheme*."

Apart from being easy to circumvent by just guessing every number between 0 and 25 (a weakness that can be mitigated by variations in how the key is used[24]), symmetric encryption schemes suffer from a fundamental limitation—the sender and receiver need to have agreed on a key in secret prior to sending the message. This is not always possible. For example, it would be impractical to encrypt a connection between a web browser and a website (say, Amazon.com) in this way because there is no way for Amazon and every one of its customers to agree on a secret key prior to making the connection. Without encrypting the connection, however, it would be impossible for customers to securely shop online with their credit cards. Anyone intercepting the connection would have access to the sensitive information.

Such encrypted connections can be established through asymmetric encryption schemes. These schemes are also called "*public key*" encryption schemes because one of the keys—the one used for encryption—is made public to the world. The decryption key is mathematically related to but separate from the encryption key and is kept private. The public and private keys together are called the "*key pair*." A sender uses the recipient's publicly available encryption key to encrypt her message, and the recipient decrypts it with his decryption key, which he has kept to himself.

---

24. *See* Ron Rivest, *6.857 Lecture 2*, MIT 1–3 (Sept. 9, 1997), http://web.mit.edu/6.857/OldStuff/Fall97/lectures/lecture2.pdf [https://perma.cc/EB9T-YSG6] (discussing "one-time pad," a generalized version of this technique that is a theoretically "unbreakable" form of encryption, at least when unlimited computing resources are available).

Although it is hard to provide a mathematically simple version of such a scheme by way of example, a physical analogy can help. Imagine that Alice wants to send a package to Bob[25] but cannot meet with him ahead of time to exchange keys to a shared lock. Instead, she calls Bob and asks him to send her a padlock to which only Bob has the key, but with the padlock in an unlocked state. When Alice receives the lock, she puts her package in a box and closes the padlock. She can't unlock the padlock at this point because she doesn't have the key. When she sends it, anyone who intercepts the package is also unable to open it. Only Bob, once he receives the package, can open the padlock and retrieve the package. Figure 1, below, illustrates the mechanics of this scheme.

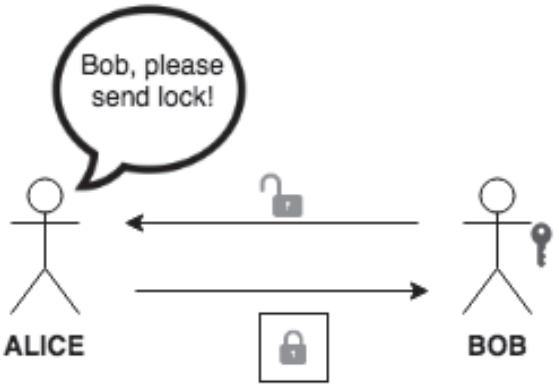

Figure 1: Illustrating how Alice can send Bob a secure package without prearranging a shared key.

Notice that in this scheme, the package remains secure even if someone is opening and inspecting (but not tampering with) Alice and Bob's mail. All that an interceptor sees initially is an unlocked padlock and then, later, a box locked with that padlock. At no point

25. For some reason, cryptography literature ubiquitously labels the sender as "Alice" and the recipient as "Bob." I adopt the convention here and take advantage of the disambiguation in the gendered pronouns. According to one source, the first use of the name was in a paper by Ron Rivest, Adi Shamir, and Leonard Adleman, the inventors of the classic "RSA cryptosystem." *See* Quinn Dupont & Alana Cattapan, *Alice & Bob, A History of the World's Most Famous Cryptographic Couple*, http://cryptocouple.com/Alice%20and%20Bob%20-%20DuPont%20and%20Cattapan%202017.pdf [https://perma.cc/V22P-L5VG]. Despite its age, RSA is still core to the iMessage encryption system (among many others). *See* APPLE, *supra* note 23, at 60.

does either the key or the unlocked box go through the mail.[26] Although the devil will always be in the technical details, this is the basic reason that two parties speaking to each other can establish a secure conversation even in the presence of an eavesdropper.

A typical messaging service offering "end-to-end encryption" looks a lot like this, but it has an additional feature: the service offering the transportation of messages is the same one that effectuates the encryption. To match the physical analogy to that arrangement, imagine that instead of Alice calling Bob on some separate channel (like a phone call) to request a padlock, FedEx were to preemptively give each of its customers a key to a unique padlock that it kept in storage and promised not to keep copies of the keys. FedEx would keep the padlocks in an unlocked state. When Alice wants to send Bob a package, she merely asks FedEx to put on "Bob's" padlock. When Bob receives his package, he can unlock the padlock with the key that only he has and give the unlocked padlock back to FedEx. As long as FedEx keeps its word about attaching the right padlock and not retaining copies of the keys, Alice and Bob can be sure that neither FedEx, nor anyone intercepting FedEx packages, will see the inside of the package.

This revised, fanciful arrangement is essentially how modern messaging services that rely on end-to-end encryption work. The service provider facilitates not just the transportation between user accounts (which, in many cases, is an account system that the service provider itself controls), but also manages the keys for its users. The private decryption keys are kept safe on the users' devices without the service provider retaining or having access to them. When one user wants to send an encrypted message to another, she asks the service provider for the recipient's public encryption key. Having encrypted the message, she sends the ciphertext over to the user, who uses his private decryption key to recover the plaintext.[27]

---

26. Of course, in the physical world, it may be possible to construct a key just from careful inspection of a padlock, but that is not the case with the mathematical system after which this analogy is modeled. Similarly, the assumption is that it is impossible (or at least intractably difficult) to simply "guess" the mathematical key in a way where one could pick a physical lock. *But see infra*, note 27 (explaining that this assumption is not proven).

27. Asymmetric encryption schemes come with a massive disclaimer, and this footnote is as good a place for it as any: they are not proven to be secure. Many different asymmetric encryption algorithms have been proposed over the years, some of which have shown themselves to be convincing enough to researchers that trillion-dollar industries have been built on the assumption that they cannot be defeated in any practical amount of time. And yet, to date, no one has been able to prove that no clever algorithm exists that can quickly recover a plaintext from a

Different implementations of end-to-end encryption schemes work differently in practice, but this illustration roughly describes them all. One important special case, particularly relevant to this Note, is Apple's iMessage. There, a user has a different key pair associated with each device she owns.[28] Thus, a user's iPhone, iPad, and MacBook all have their own decryption keys stored privately on each respective device, with the corresponding public encryption keys stored by Apple. When Alice wishes to send a text message over iMessage to Bob, Apple sends *all* of Bob's encryption keys to Alice. Alice's device sends multiple copies of the message—one for each device's encryption key—and Apple forwards them to Bob's corresponding devices for decryption.[29] That is how it is possible for Bob to see incoming messages on all of his devices, but why a newly purchased device will not show old messages (unless it was restored from a backup of an old device). Figure 2, below, illustrates how end-to-end encryption works on Apple's iMessage in the case where Bob owns just one device.

---

ciphertext encrypted with an encryption key in an asymmetric encryption scheme. Furthermore, it *has* been shown that quantum computers, if they can ever be reliably built at scale, can efficiently break a subset of commonly used asymmetric encryption schemes, including, notably, RSA (*see supra* note 25). *See generally* Stephanie Blanda, *Shor's Algorithm—Breaking RSA Encryption*, AMS BLOGS (Apr. 30, 2014), https://blogs.ams.org/mathgradblog/2014/04/30/shors-algorithm-breaking-rsa-encryption/ [https://perma.cc/FDB2-XED7]. There is a million-dollar bounty for a mathematical solution to a highly generalized version of this open problem—a figure that is laughably small compared to the economic ramifications of a proof that asymmetric encryption schemes do not, in fact, work. *See generally P vs NP Problem*, CLAY MATHEMATICS INST., http://www.claymath.org/millennium-problems/p-vs-np-problem [https://perma.cc/5C3H-TG3L]. In fact, the so-called "P-vs-NP problem" has ramifications that extend far beyond the realm of cryptography, including into logistics, *id.*, and even far-flung fields like the drawing of voting districts, Michah Altman & Michael McDonald, *The Promise and Perils of Computers in Redistricting*, 5 DUKE J. CONST. L. & PUB. POL'Y 69, 81 (2010).

In any case, this Note proceeds, as the rest of the world has, on the assumption that at least some version of asymmetric encryption schemes in use today does work and is not, crudely put, "easily breakable," at least if correctly implemented. Incidentally, it is generally understood that correct implementations are a big "if," and that in almost all cases, bugs in the implementation are what tend to cause security vulnerabilities rather than some fundamental mathematical flaw in the underlying encryption scheme. *See, e.g.*, Bruce Schneier, *Security Pitfalls in Cryptography*, SCHNEIER ON SECURITY (1998), https://www.schneier.com/essays/archives/1998/01/security_pitfalls_in.html [https://perma.cc/D97M-DPDL] (describing a variety of attack vectors having nothing to do with encryption).

28. *See* APPLE, *supra* note 23, at 60.

29. *Id.*

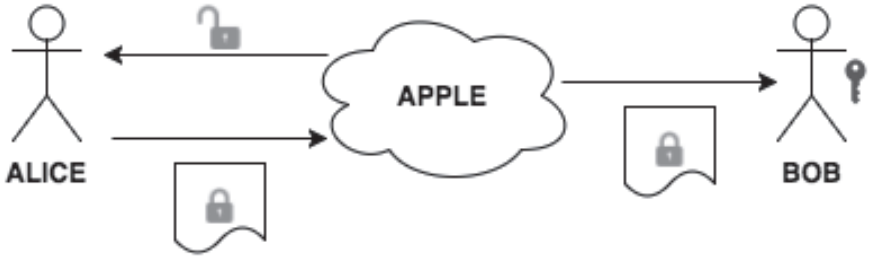

Figure 2: Illustrating how Alice can send Bob an encrypted message so Apple can't read it. The lock represents Bob's public encryption key and the key represents his corresponding private decryption key. The locked message indicates that the message is encrypted. Bob can decrypt the message with his private key when he receives it.

The next Section describes authentication, a sort of counterpart to encryption.

B. User Authentication

Encryption and decryption are not the only cryptographic operations. There are also a large number of operations that broadly fall into the category of "authentication." Unlike encryption, which is designed to ensure *secrecy*, authentication is designed to ensure *integrity*. Authentication technologies, among other things, enable senders to digitally "*sign*" their messages and allow recipients to "*verify*" those signatures. These signatures can provide various assurances, including that the message was not modified after it was sent and that the message was sent by a particular sender. This Note is primarily concerned with the latter functionality, which I call "*user authentication*."[30]

User authentication can be effectuated through asymmetric keys, just like encryption. In that context, the key that remains private is used for signing, while the key that is publicly disclosed is

30. The concept of signing and verifying messages is not limited to end-to-end communication services. Websites, for example, use the same technology to assure web browsers that they are operated by a particular real-life entity. *See generally Certificate Authorities & Trust Hierarchies*, GLOBALSIGN, https://www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies/ [https://perma.cc/SS57-LTME]. Furthermore, the exact same technology is used by Apple to protect against unauthorized updates to the iPhone operating system, which was the technology at issue in the San Bernardino controversy. *See infra* Part I.D. I chose the term "user authentication" to emphasize that this technology is what enables users to trust their counterparties' reported identities, and to distinguish from other similar authentication-related operations. It is not a term of art used in the field generally.

used for verifying. Although the standard terms, "private key" and "public key," are also used in the context of authentication schemes, I will use the non-standard terms, "signing key" and "verification key," for clarity.

As noted in the introduction, end-to-end encryption services would be of little use if the users did not know with whom they were speaking.[31] For this reason, user authentication is built into them as well. When Alice wishes to send a message to Bob, she not only encrypts her message with Bob's publicly available encryption key, but also signs it with her private signing key. When Bob receives the message, he first verifies the signature with Alice's publicly available verification key and then decrypts it with his private decryption key. As long as the users are confident that the publicly available keys in fact belong to the users they purport to belong to (or, more precisely, that the corresponding private keys were solely in the possession of those users), both the confidentiality and integrity of the system are assured.

To illustrate, suppose Alice and Bob are using iMessage to communicate. Apple maintains both users' keys in a large directory. When Alice requests Bob's key(s), she gets back a message that, in simplified form, looks something like Figure 3:

31. For this reason, I say that user authentication is necessary for end-to-end encryption to work. As the previous Section demonstrates, it is also "sufficient" because asymmetric encryption schemes enable users to create a private communication channel while speaking publicly. Thus, given a public authenticated channel (that is, where everything said is public but attributable to the speakers), asymmetric encryption can be used to enable a private conversation. In fact, as it turns out, researchers have proposed ways to maintain confidential conversations in public without using encryption (or keys) at all. One famous proposal is called "Chaffing and Winnowing." *See* Ronald L. Rivest, *Chaffing and Winnowing: Confidentiality without Encryption*, MIT LAB FOR COMPUT. SCIENCE (Mar. 18, 1998), http://people.csail.mit.edu/rivest/chaffing-980701.txt [https://perma.cc/ZPB9-894N]. Professor Ron Rivest proposed this scheme in the context of the 1990s key escrow debate. *See supra* notes 11–14 and accompanying text. However, the Chaffing and Winnowing scheme still assumes an authenticated channel because, as noted earlier, a conversation cannot be truly confidential without the parties being sure about each others' identities.

```
{
 user: "Bob",
 pubkeys: [
"12345",
"67890"
 ]
}
```

Figure 3: Illustrating a simplified example of a key transmission for user "Bob." In this example, Bob has two public keys, "12345" and "67890." These public keys are associated with two private keys, each of which is stored on a device (e.g., Bob's iPhone and iPad) and not shared with anyone else, including Apple.

The security of iMessage depends on the integrity of that directory—that is, on the assurance that the public keys listed for a particular Apple account are in fact associated with the owner of that account. The full scheme is illustrated in Figure 4, below.

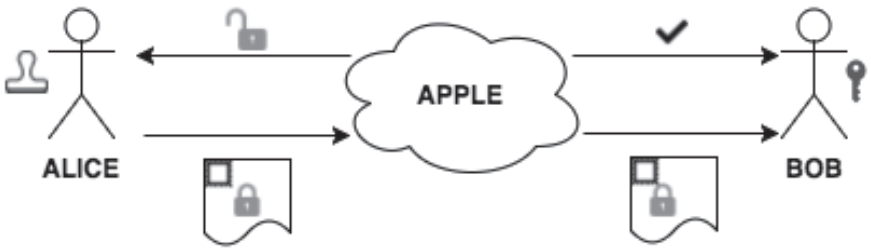

Figure 4: Illustrating the added authentication layer on top of the encryption layer. The stamp represents Alice's private signing key and the checkmark represents her corresponding public verification key. The stamped and locked message indicates that the message is encrypted with Bob's public encryption key and signed with Alice's private signing key. When Bob receives the message, he can verify it with the public verification key and decrypt it with his private decryption key.

C. The Assisted MITM Attack

As the discussions in the first two Sections demonstrate, the schemes used in many messaging services that offer end-to-end encryption actually require a great deal of trust in the service provider. First, the service provider must keep its word that the private keys are only stored on its users' devices and are not secretly copied to the service provider's servers. Apple's iMessage is proprietary software, so there is no practical way to independently verify compliance with that requirement. There are, however, some open source end-to-end messaging programs, such as Signal, where ex-

perts are able to verify that the private keys remain secure.[32] But second, and more fundamentally, encryption and authentication schemes like the ones described here require that the public keys, which the service provider sends to a user, in fact match the identity of the counterparty that they supposedly belong to. That fundamental issue of matching keys to users is broadly called "*key distribution*." An inherent weakness in any end-to-end encryption scheme that relies on a centralized directory of users for key distribution is that the service that operates the centralized directory must be trusted to always correctly identify which key belongs to which user.

Thus, because the correspondence between users and their public keys is a core requirement for all end-to-end encrypted systems, it is a source of potential vulnerabilities. If a third party were able to replace a user's public key with its own, it would undermine the system's security. Specifically, if it replaced Bob's encryption key, it would be able to decrypt messages sent to him; if it replaced Alice's verification key, it would be able to forge messages to seem as if they were written by her. The general form of this technique—intercepting communications and tampering with them before sending them on—is called a "man-in-the-middle (MITM) attack." Because this Note focuses on the government acting as the third-party interceptor, it assumes that this key replacement is accomplished through some form of legal coercion, such as a subpoena or court order, rather than by technical malfeasance. Nonetheless, to adopt the common parlance of security literature, I refer to this technique as an "attack," meaning simply an action that is intended to undermine some security guarantee. I refer to the government's coercing the service provider to assist the government as an "assisted MITM attack" and to the legal process used in the coercion (be it subpoena, court order, or otherwise) as an "assisted MITM order."

In the case of iMessage, the assisted MITM attack would work as follows. The government would generate its own encryption key pair and then send Apple an order that compels it to transmit to a sender the government's public encryption key, instead of (or along with) one belonging to the intended recipient. For example, if Bob was the target and the government wanted to read all messages sent to him, it would compel Apple to replace Bob's encryption key with the government's encryption key. Ordinarily when Alice sends Bob a message, her device would normally en-

32. *See Signal*, SIGNAL, https://signal.org/; *Signal*, GITHUB, https://github.com/signalapp [https://perma.cc/AKD5-7E3U] (containing all source code for Signal software).

crypt it with Bob's encryption key. However, because the government compelled Apple to send the *government*'s encryption key and claim it belonged to Bob, the government would be able to intercept and decrypt the message with its corresponding decryption key. To complete the attack, the government could generate a separate authentication key pair and compel Apple to claim that the government's verification key was Alice's. The government could then resend the message to Bob by signing with its own signing key. When Bob received the message, his device would ask Apple for Alice's verification key, and Apple would be compelled to give the key that was supplied by the government. Thus, it would appear as if the message came from Alice. Neither Alice nor Bob would be able to detect what happened. Figure 5, below, illustrates the complete attack.

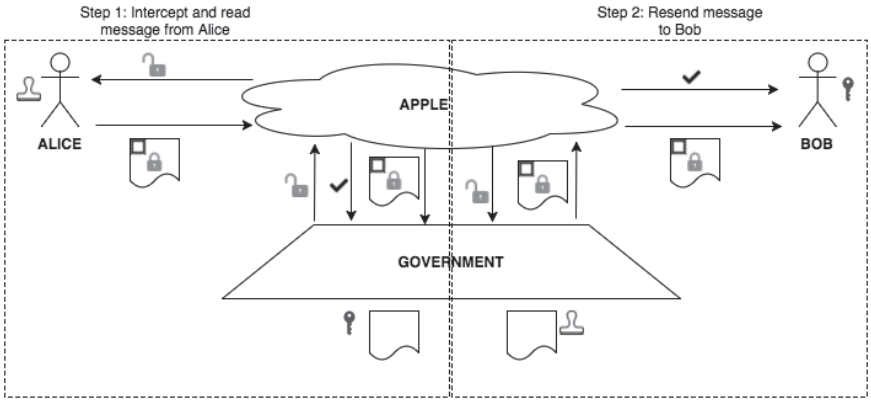

Figure 5: Illustrating the completed assisted MITM attack. The dashed rectangles represent the two steps of the process. In the first step, the government stands in the shoes of Bob. Alice receives an encryption key that she believes belongs to Bob but in actuality belongs to the government. In the second step, the government stands in the shoes of Alice. Bob receives a verification key that he believes belongs to Alice but in actuality belongs to the government. By conscripting Apple to forward the keys and represent that they belong to each party, the government is able to decrypt messages and forward them along to the other party without being detected.

As mentioned earlier, iMessage is designed so that each user can have multiple public keys (for both encryption and authentication) associated with her account: each key corresponds to a separate Apple device (on which is stored a corresponding private key). Thus, Apple has already built up the infrastructure for an even simpler version of this attack. The government's key pair would just be treated as a new "device" associated with each user account, and its

public key would appear as one of the "pubkeys" in Figure 3, above. When Alice sent a message to Bob, the government would silently get a copy. To be fair, when a new device is associated with an account, the user typically receives an alert. Thus, if the government simply added a new key to Bob's account, he may receive a warning.[33] Apple has never commented on whether it could disable that warning without alerting the user.

D. A Brief Digression on San Bernardino

Although not directly related to the topic of this Note, the extensive coverage of the 2015 San Bernardino terrorist attacks and of the subsequent controversy between Apple and the FBI make it worth taking a brief detour to explain how the issues in that case relate to the ones addressed here. Despite the presence of some of the same actors (Apple and the government) and the same themes (encryption on Apple devices, law enforcement needs, and the First Amendment), the issues are in fact very different.

The facts, briefly, are as follows. After the attack,[34] the FBI recovered a locked Apple iPhone 5C owned by one of the perpetrators. The iPhone contained encrypted content, but before the FBI could access that encrypted content, it had to unlock the iPhone by entering the suspect's passcode. The iPhone was configured to automatically delete all the contents stored on the device after 10 incorrect unlock attempts (this is an optional feature present on newer iPhone devices).[35] The FBI requested Apple's assistance in either disabling the feature or recovering the unencrypted content. Apple declined to help, and the FBI filed for and obtained a court order, issued under the All Writs Act,[36] compelling Apple's assistance. Apple appealed the order, but the litigation became moot after an unidentified entity helped the FBI recover the contents.[37]

---

33. APPLE, *supra* note 23, at 60.

34. *See generally* Michael S. Schmidt & Richard Pérez-Peña, *F.B.I. Treating San Bernardino Attack as Terrorism Case*, N.Y. TIMES (Dec. 4, 2015), https://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html.

35. *Apple-FBI Battle Over San Bernardino Terror Attack Investigation: All The Details*, L.A. TIMES (Feb. 19, 2016, 6:08 PM), http://www.latimes.com/business/technology/la-fi-tn-apple-fbi-20160219-htmlstory.html [https://perma.cc/C7C9-HP5Z].

36. *See infra* Part II.A for a detailed discussion of the All Writs Act.

37. Jack Date et al., *Justice Department Withdraws Request in Apple iPhone Encryption Case After FBI Accesses San Bernardino Shooter's Phone*, ABC NEWS (Mar. 28, 2016, 10:05 PM), http://abcnews.go.com/Technology/justice-department-withdraws-request-apple-iphone-encryption-case/story?id=37986428 [https://perma.cc/2F54-G3NN].

The validity of the AWA order has never been ultimately determined.[38]

The primary distinction between the order received by Apple in the aftermath of San Bernardino and an assisted MITM order as discussed in this Note lies in the differences between the role of encryption—and, consequently, the necessary technical assistance—in the two cases. Apple explained that just as with its iMessage service, it does not have the technical capability to directly decrypt the contents of a locked iPhone because it does not have a copy of the key used to encrypt it. It could, however, send an update to the operating system that would disable the security features, allowing the FBI to simply try all possible combinations without the device automatically erasing all of its contents after 10 incorrect attempts. One of the reasons the FBI needed Apple's assistance is that the device hardware separately required all code updates to be digitally signed (in the same sense of signing as described in Part I.B) with the verification key hardcoded into the phone itself. Only Apple has the signing key necessary to sign updates; this is a security feature that prevents malicious attackers from writing false operating system updates to take over the device.[39]

Thus, the FBI's request for assistance in the aftermath of San Bernardino is properly characterized as not only asking Apple to write code for it, but also for signing that code as, in some sense, "authentic." Part of Apple's argument against the validity of the San Bernardino order rested on a First Amendment theory that being forced to write computer code violates the First Amendment. That argument should not be confused with the discussion in Part III, which does not have to do with writing code, but rather with transmitting a particular message. The analogy to my argument would be a complaint that the order required Apple to designate the code as "authentic." Apple never made that argument, and for good reason: by signing the code it was asked to write, it would simply be attesting that the code was "genuine Apple code," which would be true. The signature would only mean that the code was written by Apple, not that Apple had a subjective desire to write it.

38. In fact, in an unrelated case, Magistrate Judge James Orenstein declined to issue a substantially identical order, finding that it was *not* appropriate under the All Writs Act. *In re* Apple, Inc., 149 F. Supp. 3d. 341, 353–75 (E.D.N.Y. 2016). Thus, the issue is in the nascent stages of a potential circuit split.

39. L.A. Times, *supra* note 35.

E. In Summary

Needless to say, cryptography is a complex subject. For the purposes of this Note, however, all that is necessary to understand is the meaning of an assisted MITM order, which is simply a court order compelling the exchange of keys as illustrated in Figure 5, above. With that, this Note proceeds to a purely legal discussion.

II.
AUTHORITY FOR ISSUING SUCH AN ORDER

To my knowledge, there is no known incident in which the government actually issued anything like an assisted MITM order.[40] However, the possibility has long been discussed in technical and public literature[41] and, as explained in the previous Part, it would not be technically difficult to implement. This Part argues that there are at least two sources of legal authority that the government could rely on when issuing an assisted MITM order.

---

40. A recent report from Reuters describes an attempt by the Department of Justice to compel Facebook to "break the encryption in its popular Messenger app," which allows users to encrypt some conversations end-to-end, including when making one-on-one calls through the program. Dan Levine & Joseph Menn, *Exclusive: U.S. Government Seeks Facebook Help to Wiretap Messenger—Sources*, REUTERS (Aug. 17, 2018 4:34 PM), https://www.reuters.com/article/us-facebook-encryption-exclusive/u-s-government-seeks-facebook-help-to-wiretap-messenger-sources-idUSKBN1L226D [https://perma.cc/RM6Z-4J9L]. The case remains under seal, so it is unknown whether the government is requesting an assisted MITM order or trying some other technique. However, Facebook is apparently arguing that "it can only comply with the government's request if it rewrites the code relied upon by all its users to remove encryption or else hacks the government's current target." *Id.* An assisted MITM attack should not require alterations to any code, although it is hard to infer too much from unattributed sources in a non-technical news article.

An arguably related fact pattern comes from two cases in Washington, apparently stemming from the same arrest, in which a police officer used a seized iPhone to impersonate the arrestee in order to arrange some drug deals in a sting operation. State v. Hinton, 319 P.3d 9 (Wash. 2014); State v. Roden, 321 P.3d 1183 (Wash. 2014). The police officer did not seek court authorization prior to sending the text messages. *Hinton*, 319 P.3d at 11; *Roden*, 321 P.3d at 1185. The Supreme Court of Washington vacated both convictions on state constitutional and statutory grounds. In both cases, the court focused on the privacy expectations of the individuals who were tricked into communicating with the police officer. *Hinton*, 319 P.3d at 17 (basing ruling off of the state constitution); *Roden*, 321 P.3d at 1189–90 (state statute). Neither of the cases addressed either Apple's interests or the interests of the owner of the iPhone who was being impersonated by the police officer. *See also* Sacharoff, *infra* note 126 (discussing listeners' interests in the context of the First Amendment).

41. *See supra* note 19.

A. The All Writs Act

The All Writs Act (AWA) grants federal courts authority to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[42] The AWA acts as a "gap-filler" that gives courts the authority to issue orders that are not expressly provided for by other laws but which are necessary to effectuate some existing authority.[43] The preexisting authority may be some inherent authority vested in the courts or derived from some statutory or constitutional authority.[44]

A watershed decision connecting the AWA to advanced electronic investigative techniques is *United States v. New York Telephone Company*.[45] There, a court in the Southern District of New York found probable cause to issue an order that authorized FBI agents to install a "pen register"[46] to monitor several phone lines operated by the New York Telephone Company. The order, issued under the AWA and Rule 41 of the Federal Rules of Criminal Procedure, directed the company to assist the agents in installing the pen registers and the FBI to compensate the company for its efforts.[47] The company declined to comply with the order, arguing that such an order could only be issued through the special procedures established by the Wiretap Act.[48] The Second Circuit determined that pen registers do not fall under the scope of the Wiretap Act and that the district court had the authority to issue such an order under Rule 41 and the AWA.[49] The Second Circuit concluded, however, that the district court abused its discretion in ordering the company to offer technical assistance.

---

42. 28 U.S.C. § 1651(a) (2012).

43. *See* Brian M. Hoffstadt, *Common-Law Writs and Federal Common Lawmaking on Collateral Review*, 96 NW. U. L. REV. 1413, 1460–61 (2002).

44. *See, e.g.*, Harris v. Nelson, 394 U.S. 286, 299 (1969) (holding that the AWA confers a power to hold evidentiary hearings in connection with habeas corpus proceedings based on "[the presence] of habeas corpus jurisdiction and the duty to exercise it").

45. 434 U.S. 159 (1977).

46. *Id.* at 161. "A pen register is a mechanical device that records the numbers dialed on a telephone . . . [without] . . . overhear[ing] oral communications. [It] does not indicate whether calls are actually completed." *Id.* at 161 n.1.

47. *Id.* at 161.

48. *Id.* at 163. The Wiretap Act refers to Title III of the Omnibus Crime Control and Safe Streets Act of 1968. *See In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 135 (3d Cir. 2015) ("The federal Wiretap Act is codified at 18 U.S.C. § 2510 *et seq.*"); Pub. L. 90-351, 82 Stat. 212.

49. 434 U.S. at 164.

The Supreme Court upheld the order in full. The Court agreed that the Wiretap Act does not cover pen registers[50] and found that to the extent that the Federal Rules of Criminal Procedure do not explicitly confer the ability, the AWA fills the gap.[51] Furthermore, the Court found that the district court did not abuse its discretion because "the [c]ompany was a third party [not] so far removed from the underlying controversy that its assistance could not be permissibly compelled."[52] The Court found it significant that a district court found probable cause of a "criminal enterprise" which was potentially using "the [c]ompany's facilities . . . on a continuing basis."[53] It also emphasized that the company would be compensated for its assistance and that "compliance with [the order] required minimal effort on the part of the [c]ompany and no disruption to its operations."[54]

Although the analog telephonic technology at issue in *New York Telephone* is very different from digitally-encrypted messages sent over the Internet, the legal analysis of the AWA remains the same. Apple is in an analogous position to the New York Telephone Company and the effort needed to effectuate an assisted MITM order would be minimal. The Supreme Court in *New York Telephone* pointed out that the company "regularly employs such devices without court order"[55] for various reasons. Apple similarly already has infrastructure for associating new keys with user accounts (such as when users purchase new devices), and there is no technical reason why Apple could not simply include a different key proposed by the government.[56] In other words, although the technical issues are different, the question of the powers of a court as conferred by the AWA are essentially identical.[57] The AWA would confer the necessary authority for a court to issue an assisted MITM order.

---

50. *Id.* at 165–68.

51. *Id.* at 168–70.

52. *Id.* at 174.

53. *Id.*

54. *Id.* at 175.

55. 434 U.S. at 174.

56. *See supra* Part I.C.

57. One distinction between an assisted MITM attack and the pen register in *New York Telephone* is that, depending on how the MITM attack was carried out, ongoing assistance from Apple may be required. The Ninth Circuit held that this distinction is not sufficient to defeat the authority conferred by the AWA. *See In re* Application of the United States for an Order Auth'ing an In-Progress Trace of Wire Commc'ns over Tel. Facilities, 616 F.2d 1122, 1130 (9th Cir. 1980).

B. The Stored Communications Act

The Stored Communications Act (SCA)[58] addresses requirements for third-party service providers who store electronic data that belongs to their subscribers.[59] It proscribes voluntary disclosure of user data under some circumstances[60] and provides various levels of protection for compelled disclosure, depending on the service and the type of data requested.[61] Furthermore, the SCA allows a court to issue a "gag order" that prevents the service provider from notifying its subscriber that the provider was issued, or responded to, a data request.[62]

The SCA makes a distinction between "electronic communication services" and "remote computing services." The former refers to "any service which provides to users thereof the ability to send or receive wire or electronic communications,"[63] whereas the latter refers to "the provision to the public of computer storage or processing services by means of an electronic communications system."[64] An "electronic communications system," in turn, is defined as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[65] The term "electronic storage" is specifically defined to include "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."[66] And finally, the term "electronic communication" is defined to include "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system," but not analog audio

58. 18 U.S.C. §§ 2701–2712 (2012).

59. The SCA is actually Title II of the Electronic Communications Privacy Act, which in turn was an amendment to the Wiretap Act (Title III of the Omnibus Crime Control and Safe Streets Act of 1968). *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510–22*, JUSTICE INFO. SHARING, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 [https://perma.cc/B9HB-GJYX]. Recall that the New York Telephone Company argued that the order compelling its help could not be issued under the AWA because it was foreclosed by the Wiretap Act.

60. *See* § 2702(a).

61. *See* § 2703.

62. *See* § 2705(b).

63. § 2510(15).

64. § 2711(2).

65. § 2510(14).

66. § 2510(17)(A).

communications, communications from tone-only paging devices or mobile tracking devices, or electronic fund transfers.[67]

It is difficult to say with certainty how these 1980s-era concepts should apply to twenty-first century technologies. Most modern Internet-enabled communication services could probably be characterized as either electronic communications services or remote computing services, depending on which application is at issue.[68] Regardless, the requirements of section 2703 would govern compelled disclosure of user data. A message stored for 180 days or less—which would include messages sent via iMessage, since Apple only keeps encrypted messages for one month[69]—can only be disclosed "pursuant to 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."[70] Messages stored longer than that can also be requested by court order or subpoena.[71]

Thus, to the extent the SCA modifies the landscape since *New York Telephone*, it provides the necessary substrate to which the AWA can be applied. An order issued under section 2703 for "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less" clearly describes a message in transit, given that storage incidental to a transmission is included in the definition of "electronic storage."[72] Additionally, section 2706, which allows for reimbursement for services complying with governmental orders, specifically includes reimbursement for "such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information."[73] The broad language comfortably includes decryption, since decryption would be a required step in "assembling, reproducing, or otherwise providing" the messages. The SCA therefore most likely also provides courts with the authority necessary to issue an assisted MITM order, at least in the context of decryption.

---

67. § 2510(12).

68. *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980–91 (C.D. Cal. 2010) (concluding that social networking sites could be treated as either electronic communication services or remote computing services, depending on how they were being used).

69. APPLE, supra note 23, at 62.

70. § 2703(a).

71. § 2703(b).

72. *See supra* note 66 and accompanying text.

73. § 2706(a).

C. The Burr-Feinstein Legislation

In the wake of the 2015 San Bernardino attacks and the resulting controversy between FBI and Apple,[74] Senators Richard Burr and Dianne Feinstein introduced legislation that would have implicitly granted authority for an assisted MITM order (as well as the order sought by the FBI to compel Apple to assist the FBI in accessing the suspect's locked iPhone following the San Bernardino Attacks).[75] The bill, whose short title was "Compliance with Court Orders Act of 2016,"[76] would have required that "a covered entity that receives a court order from a government for information or data shall provide such technical assistance as is necessary to obtain such information or data in an intelligible format or to achieve the purpose of the court order."[77] The term "covered entity" was defined to mean "a device manufacturer, a software manufacturer, an electronic communication service, a remote computing service, a provider of wire or electronic communication service, a provider of a remote computing service, or any person who provides a product or method to facilitate a communication or the processing or storage of data."[78] That expansive definition would easily include Apple as well as any other provider of messaging software.

Although the Burr-Feinstein legislation was specifically written to address Apple's non-compliance with the FBI's request in the wake of the San Bernardino attacks,[79] which is different from the vulnerability discussed here, the legislation was not limited to that context. First, the bill repeatedly refers to "communications services" as one of its primary targets.[80] Even more telling, the bill defines "technical assistance"—which the covered entities, including providers of communication services, must render—to include *either* delivering data in an intelligible format "concurrently with its transmission" *or* "expeditiously, if stored by a covered entity or on a

74. *See supra* Part I.D.

75. S. ___, 114th Cong. (2016) (discussion draft) [hereinafter Burr-Feinstein], https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf [https://perma.cc/AQR8-P3BK].

76. *Id.* § 1.

77. *Id.* § 3(a)(1).

78. *Id.* § 4(4).

79. *See* Dustin Volz & Mark Hosenball, *Senate Proposal on Encryption Gives Judges Broad Powers*, REUTERS (Mar. 21, 2016, 6:22 PM), http://www.reuters.com/article/us-apple-encryption-legislation/senate-proposal-on-encryption-gives-judges-broad-powers-idUSKCN0WN2B1 [https://perma.cc/4YQ9-LKN5] (discussing the legislation in the context of the San Bernardino attacks).

80. *See* Burr-Feinstein §§ 2(4), 3(e), 4(4), 4(6).

device."[81] In other words, the legislation foresaw *both* a case analogous to San Bernardino—where the information was already stored on the device—*and* a situation where the information is being transmitted in real time. Although the bill does not explicitly authorize a prophylactic approach like an assisted MITM order, any "assistance" to obtain decrypted information of data "concurrently with its transmission" would presumably require some work on the part of the communications service provider prior to the transmission of the data. Thus, the legislation would have almost certainly authorized an assisted MITM order.

One could argue that the fact that the Burr-Feinstein legislation was proposed and ultimately rejected[82] suggests that Congress has not authorized assisted MITM orders under existing statutes, including the AWA or SCA. For the reasons already described in the preceding sections of this Part, I reject that view. Additionally, Burr-Feinstein was proposed soon after Magistrate Judge James Orenstein concluded, in a separate but factually indistinguishable case, that the AWA does not supply courts with the authority to grant the order the FBI was requesting after San Bernardino.[83] The case was widely publicized due to its conflict with the order authorized by the federal court in California.[84] Thus, it is much more likely that the Burr-Feinstein bill was introduced simply to foreclose any doubt about the AWA in that very novel context. The assisted MITM order setting, although incidentally affected, is in some sense much more similar to other existing wiretap techniques.

III.
THE RIGHTS OF THE SERVICE PROVIDERS

An assisted MITM order conscripts service providers (who are essentially third parties to government surveillance) and, as I elaborate below, forces them to lie. This Part argues that this aspect of the technique is constitutionally fatal because it violates the service providers' First Amendment rights.

---

81. *Id.* § 4(12).

82. *See* Dustin Volz et al., *Push for Encryption Law Falters Despite Apple Case Spotlight*, REUTERS (May 27, 2016, 7:46 AM), http://www.reuters.com/article/usa-encryption-legislation/push-for-encryption-law-falters-despite-apple-case-spotlight-idUSL2N18O0BM [https://perma.cc/BF7K-ETBF].

83. *See supra* note 38.

84. *See, e.g.*, Katie Benner & Joseph Goldstein, *Apple Wins Ruling in New York iPhone Hacking Order*, N.Y. TIMES (Feb. 29, 2016), https://www.nytimes.com/2016/03/01/technology/apple-wins-ruling-in-new-york-iphone-hacking-order.html [https://perma.cc/QP6R-U37E].

A. The Exchange of Cryptographic Keys is Speech Under the First Amendment

A threshold question is whether the mandated exchange of cryptographic keys counts as "speech" for First Amendment purposes. As explained in Part I, cryptographic keys are simply very large numbers, inherently meaningless and in some interfaces, including iMessage, not even displayed to the user. One could argue, therefore, that cryptographic keys are not speech because they are not expressions that are readily comprehensible to the communicating users. This argument is unavailing for several reasons.

First, the communication is not simply that of a cryptographic key, but rather a statement *about* the key—namely, that it belongs to a particular user. When Alice sends a message to Bob, Apple supplies her with a public encryption key that it promises (for example, through its marketing materials[85]) will encrypt her message in such a way that only Bob can read it. As explained in Part I, the technology that enables this requires an associated private decryption key that only Bob has access to, and as illustrated in Figure 3 of Part I.B, the communication explicitly ties the key to the user. Thus, because Bob has exclusive control of the private key, the public key associated with it is necessarily tied to Bob as well. Although the public key is not particularly meaningful to Alice as a number, the attestation about its association with Bob is.

Second, the Supreme Court has adopted a very expansive view of what counts as speech. For example, in *Expressions Hair Design v. Schneiderman*, the Court unanimously ruled that a New York provision that prohibited merchants from imposing a surcharge on customers paying with credit cards—but allowed the economically equivalent practice of describing the price differential as a discount to customers paying by cash—was speech for the purposes of the First Amendment.[86] The communication in *Expressions Hair Design* were simply price stickers—numbers solely communicating a price. Similar to price stickers, which are used to communicate a price, cryptographic keys are used to communicate the identity of parties exchanging messages. Thus, cryptographic keys fit within this expansive interpretation of the right to freedom of speech because the exchanging of keys communicates information regarding party identity.

---

85. As an example, consider Apple's publicly available document that describes the security features of its iOS devices. *See* APPLE, supra note 23.

86. 137 S. Ct. 1144, 1147 (2017).

It is hard to distinguish numbers that communicate a price with numbers that communicate a cryptographic key, but the biggest differentiating factor, and the one alluded to earlier, is that users do not "understand" the cryptographic key, while they do "understand" a price. This line of reasoning—that whether a communication should count as "speech" turns on its understandability to humans—has been examined in a different line of cases concerning computer code. Although computer code is not the same as cryptographic keys—and I do not here argue that writing code always constitutes speech—cryptographic keys, like some computer code, are speech because they communicate an idea. For example, in *Universal City Studios, Inc. v. Corley*, the Second Circuit reviewed an order, issued under the Digital Millennium Copyright Act, enjoining web site owners from posting computer software that allowed users to play movies on DVDs on devices that were not specially licensed by manufacturers.[87] In comparing computer programs to musical notes, the court held that computer code is speech covered by the First Amendment because it can be used as a means to communicate information between specialists.

Similarly, in *Junger v. Daley*, the Sixth Circuit determined that the fact that computer code can communicate information entitles it to First Amendment protection.[88] There, a law school professor appealed a determination that certain software he wanted to publish was subject to restrictions under the Export Administration Regulations.[89] In reversing the district court's grant of summary judgment against the professor, the court held that software is protected by the First Amendment because it can be used to communicate ideas.[90] "'[A]ll ideas having even the slightest redeeming social importance,' including those concerning 'the advancement of truth, science, morality, and arts' have the full protection of the First Amendment," the court pronounced.[91]

Both the *Corley* and *Junger* courts noted the fact that computer code comes in two forms: "object code" and "source code." Object code is code that a physical computer can directly process. A computer ultimately processes electrical signals, and object code is just a representation of those signals. Source code, meanwhile, is a set of instructions written in higher-level concepts intended to be under-

87. 273 F.3d 429 (2d Cir. 2001).

88. 209 F.3d 481 (6th Cir. 2000).

89. *Id.* at 483–84. Coincidentally, the software at issue happened to be encryption software. *Id.* at 483.

90. *Id.* at 485.

91. *Id.* at 484 (quoting Roth v. United States, 354 U.S. 476, 484 (1957)).

stood by human programmers. Source code is not directly interpretable by a computer and must instead be translated into object code by specialized software.[92] The exact relationship between source code and the resulting object code, as well as the translation process between the two, varies across programming languages and operating systems. The reason that the distinction matters, however, is that object code is usually generated by, and processed by, computers and not humans. Similarly, cryptographic keys are usually processed by software and not directly used by humans. Nonetheless, although both *Corley* and *Junger* based their First Amendment holdings on the fact that computer code can be used to communicate ideas between programmers, neither confined its holdings to source code. *Corley*, for example, explicitly refused to distinguish code based on whether or not it is executable (i.e., object code). "[T]he fact that a program has the capacity to direct the functioning of a computer does not mean that it lacks the additional capacity to convey information, and it is the conveying of information that renders instructions 'speech' for purposes of the First Amendment."[93] While acknowledging that "it would be inconvenient, inefficient and, for most people, probably impossible to" program in object code,[94] courts have nonetheless accepted that the code still "communicates" those instructions and thus should not lose protection, just as a poem translated into Sanskrit should not lose protection just because few understand the language.[95] Similarly, in a copyright case, the Ninth Circuit has held that object code can "be copyrighted as expression" and that object code "also contains ideas."[96] Likewise, cryptographic keys, which, like object code, are usually meaningless to humans, are nevertheless "expression[s]" that "contain ideas."

The fundamental problem of drawing a constitutional line between source code and object code is that the latter "is merely one additional translation of speech into a new, and different, language."[97] This encapsulates the reason that the exchange of crypto-

92. *See id.* at 483. *See generally* Daniel Lin et al., *Source Code Versus Object Code: Patent Implications for the Open Source Community*, 18 SANTA CLARA COMPUTER & HIGH TECH. L.J. 235, 238–39 (2002).

93. 273 F.3d at 447.

94. *Id.* at 439.

95. *Id.* at 446.

96. Sony Comput. Entm't, Inc. v. Connectix Corp., 203 F.3d 596, 602 (9th Cir. 2000).

97. United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1126 (N.D. Cal. 2002). Elsewhere, I have argued a similar point, suggesting that the line between the two is elusive and is based less on whether the code is "executable" and more on how

graphic keys must be considered "speech" as well. Consider the simple shift-cipher discussed in Part I.A. If a recipient sees the message "MJQQT," the information that the letters were shifted up by 5 letters is incredibly meaningful. Without a communication to inform the recipient of the shift-cipher, the recipient has no way of comprehending the ideas expressed in the message—i.e., that the message is intended to read "HELLO." It is, to borrow the analogy, akin to teaching someone enough Sanskrit to understand a previously incomprehensible poem. "The letters were shifted up by 5 letters"—or, equivalently, "the key is 5"—is clearly speech for First Amendment purposes because it communicates information. To be sure, cryptographic keys are generally far larger, are used as inputs into far more complex algorithms, and are not intended to be referenced by humans. But neither is object code. The point is that both do carry a particular meaning. For cryptographic keys, that meaning is quite literally the information needed to understand a message already sent.

In a footnote in *Corley*, the Second Circuit cautioned that "in the rare case where a human's mental faculties do not intercede in executing the instructions, we have withheld protection."[98] Courts that have followed this doctrine have relied on this dichotomy that is subtly different from the object-vs-source code dichotomy. If the *recipient* of the code is only the computer—that is, if the communicators are computers—no First Amendment protection should be extended. This dichotomy covers cryptographic keys more cleanly. Because the users are not personally plugging the keys into the cryptographic algorithm, the keys should not count as communications covered by the First Amendment. This would presumably also distinguish the shift-cipher scenario.

The problem with this reasoning is that cryptographic keys *are* used by humans, or at least could be in some common scenarios. For example, although Apple does not show its users the public keys associated with the people they are talking to, many competing products, including Facebook's WhatsApp, do.[99] The purpose of

---

expressive the language is. Leonid Grinberg, *The Generativity of Programming Languages: Why "Open Source" Is About Expressive Power*, THE FUTURE OF THE INTERNET BLOG (Aug. 12, 2013), http://blogs.harvard.edu/futureoftheinternet/2013/08/12/the-generativity-of-programming-languages-why-open-source-about-expressive-power/.

98. *Corley*, 273 F.3d at 448 n.20.

99. *See End-To-End Encryption*, WHATSAPP, https://faq.whatsapp.com/en/android/28030015/ [https://perma.cc/FB2F-3XBE] (describing the "Verify Security Code" feature, which shows a number derived from the security keys). Similarly, many modern browsers display a graphic, often a green lock, to indicate that the

displaying the keys to users is to allow them to visually compare the keys across time and ensure they do not change. For example, if Alice and Bob want to use WhatsApp to secretly communicate, they could meet up in person and visually compare the keys displayed by WhatsApp. Afterwards, when they are no longer next to each other, either one can look at the displayed key and ensure that they are still speaking with the same person. Thus, although neither Alice nor Bob is manually plugging the other's key into the encryption/decryption algorithm, each is still very much relying on the key as a communication about the person she or he is speaking with.

Furthermore, whether keys are being manually plugged into an algorithm is a very brittle, and ultimately unworkable, line on which to base a constitutional judgment. For one thing, what is mathematically difficult for one person is easy for another. It would be time-consuming to decrypt a message by hand when it has been encrypted with an industry-strength encryption scheme, but it would certainly be possible. Only one decryption operation needs to be performed for a given message, so while it would take a fair amount of time, it would be significantly more practical to decrypt a message by hand—even one encrypted with a large key—than for a user to try to manually read or write object code, which might involve hundreds of millions, if not billions, of operations. Moreover, if a user *herself* writes the software to perform the decryption—after all, the specifications are publicly available and relatively straightforward to implement, even for students[100]—would that destroy her constitutional credibility as a bona fide "participant" in the cryptographic exchange?

Moreover, as the *Corley* court noted, "even dry information, devoid of advocacy, political relevance, or artistic expression, has been accorded First Amendment protection."[101] Several years later, in *Sorrell v. IMS Health Inc.*, the Supreme Court held that information about physicians' preferences in issuing prescription was speech covered by the First Amendment.[102] "Facts," explained the Court,

---

connection to the website is secured. *See, e.g.*, *How Do I Tell If My Connection to a Website Is Secure?*, MOZILLA, https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure [https://perma.cc/MVU9-2DX3].

100. *See, e.g.*, Scott Aaronson, *6.080/6.089 Lecture 17*, MIT OPENCOURSEWARE at 2–6 (Apr. 15, 2008), https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-045j-automata-computability-and-complexity-spring-2011/lecture-notes/MIT6_045JS11_lec14.pdf [https://perma.cc/NY65-KGDD] (providing and explaining two well-known public-key encryption algorithms in a computer science undergraduate class).

101. 273 F.3d at 446.

102. 564 U.S. 552, 570 (2011).

"are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs."[103] Since *IMS Health*, the Court has continued embracing an aggressive view of First Amendment protections, including for purely factual information. For example, it recently invalidated a town's "sign code"—which had differing provisions for signs directing the public to non-profit group meetings as opposed to signs covering other messages—under a strict scrutiny analysis.[104]

To reiterate, the communications containing cryptographic keys are not just numbers. They are statements of fact sent by the service provider indicating that a particular message was sent by a particular user. The key that Apple sends to the sender's device—a key that it says belongs to a particular user, but, in reality, belongs to the government—is sent with the imprimatur of Apple, Inc. It is, in the parlance of security engineers but also quite literally, an *attestation* about the message and its security guarantees. This attestation is sent every single time Apple delivers a message from Alice to Bob. Each time Bob sees a little blue bubble[105] with Alice's name at the top of the screen, Apple has communicated to Bob that Alice sent that message.

There is, in other words, a reputational element at stake. Apple's communication to Bob—that the message Bob received is from Alice—acts like a signature or a seal. Any system of verification is only as good as the verifier's word. And the evils of a compelled lie extend beyond even financial harms. If the government forced a prestigious university to print a fake diploma and transcript for an undercover agent, that may impose financial costs on the university, but it would have a more fundamentally damaging effect as well. The diploma from the university would simply *mean less*. The right not to be compelled to cheapen that meaning is protected by the First Amendment.

---

103. *Id.*

104. 135 S. Ct. 2218, 2227 (2015).

105. In the iMessage interface, messages displayed on a blue background indicate that they were sent over the iMessage service, complete with the security guarantees of the service. In contrast, messages displayed on a green background were sent on the "short message service" (SMS), which is the standard "texting" protocol that features no security guarantees. *See generally About iMessage and SMS/MMS*, APPLE, https://support.apple.com/en-us/HT207006 [https://perma.cc/RX39-XQAU]; Adam Fendelman, *Explaining SMS Messaging and Its Limitations*, LIFEWIRE (May 21, 2018), https://www.lifewire.com/definition-of-sms-text-messaging-578676 [https://perma.cc/7HG9-ZC2H].

B. Compelled Speech Triggers Strict Scrutiny

Having established that the exchange of cryptographic keys constitutes speech, I now argue that compelling a service provider to make false attestations about key ownership triggers strict scrutiny under the compelled speech doctrine.

Although many of the most grandiose utterances about the First Amendment's guarantees securing freedom of speech concern specifically limitations on the government's ability to *restrict* speech,[106] the First Amendment just as surely limits the government's ability to *compel* it. This principle was emphasized in *West Virginia Board of Education v. Barnette*,[107] which, in overruling an opinion issued just three years prior, held that the First Amendment bars a public school from compelling students to salute the American flag.[108] The Court's pronouncement that the First Amendment prevents the government from compelling students to salute the flag—and thus express a particular viewpoint,[109] even if it may be unpopular—remains one of the most enduring passages about the First Amendment: "If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion *or force citizens to confess by word or act* their faith therein."[110]

The compelled communication that would be at issue if the government issued an assisted MITM order is the service provider's attestation regarding key ownership. Private keys are by definition private to a particular account, which is to say a particular *identity*; sending a public key and promising that it corresponds to a particular private key amounts to promising that the public key belongs to the identity of the private key holder. While these communications

106. *E.g.*, Citizens United v. FEC, 558 U.S. 310, 356 (2010) ("The First Amendment confirms the freedom to think for ourselves."); Texas v. Johnson, 491 U.S. 397, 414 (1989) ("If there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable."); Bose Corp. v. Consumers Union, Inc., 466 U.S. 485, 503–04 (1984) ("The First Amendment presupposes that the freedom to speak one's mind is not only an aspect of individual liberty—and thus a good unto itself—but also is essential to the common quest for truth and the vitality of society as a whole.").

107. 319 U.S. 624 (1943).

108. *Id.* at 642.

109. No one disputed that the flag salute was an expressive act that implicated the First Amendment. *Id.* at 632 ("There is no doubt that, in connection with the pledges, the flag salute is a form of utterance.").

110. *Id.* at 642 (emphasis added).

may not be of the same character as a forced confession of loyalty to a nation or its flag, they are real, factual statements about the identity of the parties in communication. These communications are therefore analogous to the relatively "technical speech" that, although having no relation to politics, religion, or other personal viewpoints, is protected by the First Amendment. The compelled utterance of this drier, technical speech is as strictly scrutinized as political speech.[111]

In *Hurley v. Irish-American Gay, Lesbian and Bisexual Group*,[112] the Court explained that the right to be free from compelled speech "applies not only to expressions of value, opinion, or endorsement, but equally to statements of fact the speaker would rather avoid."[113] By way of example, one of the cases that the Court cited was *Riley v. National Federation of the Blind of North Carolina, Inc.*,[114] which struck down a statute that required fundraisers to "disclose to potential donors, before an appeal for funds, the percentage of charitable contributions collected during the previous 12 months that were actually turned over to charity."[115] The Court struck down the statute as an unconstitutional regulation of free speech, explaining that "[m]andating speech that a speaker would not otherwise make necessarily alters the content of the speech,"[116] and that although there is "some difference between compelled speech and compelled silence" that "difference is without constitutional significance, for the First Amendment guarantees 'freedom of speech,' a term necessarily comprising the decision of both what to say and what *not* to say."[117] The Court has continued to embrace this jurisprudence: for example, in *National Institute of Family & Life Advocates v. Becerra*, the Court partially relied on *Riley* in applying strict scrutiny to examine a California law that imposed certain disclosure requirements on so-called "crisis pregnancy centers."[118]

---

111. S*ee, e.g.*, Pac. Gas & Elec. Co. v. Pub. Utils. Comm'n, 475 U.S. 1, 16 (1986) (finding that a public commission may not require an electric company to include newsletters from a consumer advocacy organization in envelopes sent to customers).

112. Hurley v. Irish-American Gay, Lesbian and Bisexual Grp., 515 U.S. 557 (1995).

113. *Id.* at 573.

114. 487 U.S. 781 (1988).

115. *Id.* at 795.

116. *Id.*

117. *Id.* at 796–97.

118. *See* Nat'l Inst. Family & Life Advocates v. Becerra, 138 S. Ct. 2361, 2371 (2018).

These precedents make clear that the applicable level of scrutiny does not depend on whether speech is restricted or compelled, nor on how political or opinionated it is. Instead, it depends on the purpose of the regulation and the type of speech at issue (for example, commercial speech typically enjoys less scrutiny than non-commercial speech[119]). And although the speech in the assisted MITM attack may be dry and technical, First Amendment protections for purely factual speech remain quite high. Thus, if the exchange of cryptographic keys is speech for the purposes of the First Amendment—as I argue it is in the previous Section—then a compelled assertion like the one in an assisted MITM attack is unquestionably a content-based compulsion of speech. After all, it requires the provider to alter the substance of its communication to the recipient of a message by compelling the service provider to falsely attest that a particular user sent the message, when in fact the government sent the message. Content-based restrictions on speech almost always call for strict scrutiny.[120] Furthermore, none of the various exceptions that occasionally reduce judicial scrutiny of content-based restrictions or regulations apply.[121] A key exchange is not commercial speech.[122] Nor is an assisted MITM order primarily a non-speech-related order that happens to incidentally affect speech, since the actual substance of the order is to generate

119. *See generally* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 562–66 (1980).

120. *See, e.g.*, *id.* at 2226.

121. Of course, a comprehensive analysis of every possible exception to boilerplate strict scrutiny First Amendment doctrine would fill a treatise, but one helpful summary was recently published by the Congressional Research Service. KATHLEEN ANN RUANE, CONG. RESEARCH SERV., FREEDOM OF SPEECH AND PRESS: EXCEPTIONS TO THE FIRST AMENDMENT (2014), https://fas.org/sgp/crs/misc/95-815.pdf [https://perma.cc/67Z9-CT35].

122. *See, e.g.*, Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 561 (1980) (defining "commercial speech" as "expression related solely to the economic interests of the speaker and its audience"); *see also* Victor Brudney, *The First Amendment and Commercial Speech*, 53 B.C. L. REV. 1153, 1154–61 (2012) (proposing various definitions of commercial speech). Professor Brudney separates commercial speech into a "narrow" category that merely describes a proposed transaction, and an "enriched" category that contains additional expression that would otherwise be "ordinary" speech (*e.g.*, a description of how great some product or lifestyle is) but is attached to a proposed transaction. Apple's whitepaper about its products' security, *see* APPLE *supra* note 23, might fall into this latter category. However, the actual communication of the keys would not be commercial speech under either definition, since it is entirely divorced from any kind of transaction; indeed, the one relevant commercial transaction—the purchase of an Apple product—must have already occurred for the conversation to be taking place over iMessage at all.

speech (in the form of falsely attributing a key to a user). It is, quite simply, speech that is being compelled as part of a particular regulatory framework. Regardless of whether or not the government is allowed to compel such speech in a particular situation, compelling a service provider to make a particular attestation invariably triggers strict scrutiny.

C. The Routine Use of an Order Compelling Attestations About Cryptographic Keys Cannot Survive Strict Scrutiny

Of course, First Amendment protection does not render all restrictions on a communication impermissible. Under strict scrutiny analysis, restrictions on speech are allowed if they are imposed for compelling government purposes and are narrowly tailored towards fulfilling those purposes.[123] It would be impossible to say here that *no* application of an assisted MITM order in any circumstance would be impermissible. I argue merely that it is impermissible as a matter of routine police practice.[124]

There is no dispute that the government's interest in law enforcement is a compelling interest. The real question is whether this type of regulation is sufficiently narrowly tailored. Although it comes in a very different context, a rich body of case law involving compelled speech against the backdrop of compelling government interests appears in the context of mandatory disclosure requirements. The most important differentiating factor is that in the con-

123. *Reed*, 135 S. Ct. at 2231.

124. For brevity's sake, I focus here on criminal investigations rather than on national security missions. Of course, action based on national security are not immune to First Amendment restrictions, and courts have occasionally stricken down such actions on constitutional grounds. *See, e.g.*, New York Times Co. v. United States, 403 U.S. 713 (1971) (per curiam) (upholding newspapers' rights to publish the Pentagon Papers notwithstanding national security concerns). That said, I concede that the analysis in this Section would likely change in a national security context where the government interest is higher, and courts tend to accord the executive much greater deference. *See, e.g.*, In re National Security Letter, 863 F.3d 1110 (9th Cir. 2017) (finding that a non-disclosure requirement issued with a National Security Letter withstood strict scrutiny). That said, it is also worth noting that, as a practical matter, techniques used for national security are rarely used for ordinary criminal investigations. Office of the Inspector General, U.S. Department of Justice, A Special Inquiry Regarding the Accuracy of FBI Statements Concerning Its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation 4 n.3 (March 2018), https://oig.justice.gov/reports/2018/o1803.pdf [https://perma.cc/E7V7-2YH8] (explaining that internal Department of Justice policies require stringent procedures for using national security techniques for criminal cases, and noting that a relatively high-level FBI official was only aware of two instances between 2002 and 2015 when the procedures had to be invoked).

text of an assisted MITM order, the compelled speech (that the key being sent belongs to the identified user) is unequivocally false. And although I am not aware of any case that has explicitly said that false compelled speech is more suspect than truthful compelled speech, that inference can be drawn from one of the most basic justifications for free speech: that free speech facilitates the finding of truth.[125] Alternatively, Professor Laurent Sacharoff has argued that the doctrine against compelled speech is best understood as protecting the *listener's* interests rather than the speaker's.[126] Considered through the lens of the listener, traditional justifications for free speech, including the search for truth and the promotion of the marketplace of ideas, become even clearer.[127] Compelling service providers to falsely attribute keys to its users directly conflicts with this justification for free speech because the "listener," the recipient of the message, is being tricked into believing that he is communicating with a particular person, when in fact he is communicating with the government.

Furthermore, cases involving mandatory disclosure requirements illustrate the importance of protecting the communication of truthful information. For example, in *Zauderer v. Office of the Disciplinary Counsel of the Supreme Court of Ohio*,[128] the Court partially upheld a disciplinary sanction imposed on an attorney for his advertisements. In particular, although the Court found that certain rules proscribing the use of illustrations in attorney advertise-

125. *See generally* Kent Greenawalt, *Free Speech Justifications*, 89 COLUM. L. REV. 119, 130–41 (1989). Given this justification, and the recognition that national security letter (NSL) non-disclosure requirements can withstand strict scrutiny, *see supra* note 124, an interesting question arises as to the legal efficacy of "warrant canaries." A "warrant canary" is a message periodically issued by a technology company that foresees receiving an NSL at some point in the future. The message says something to the effect of "this company has not yet received an NSL [or a similar warrant or court order]." The idea is that once a company receives an NSL, it will quietly remove the message, "killing the canary in the coal mine" and silently signaling that an NSL was received without *technically* violating the nondisclosure provision. A recent paper suggested that an injunction prohibiting the removal of a canary would be more suspect than the provision itself because it would be compelling false speech. *See* Naomi Gilens, Note, *The NSA Has Not Been Here: Warrant Canaries as Tools for Transparency in the Wake of the Snowden Disclosures*, 28 HARV. J. L. & TECH. 525, 540 (2015). For what it's worth, however, that article was written prior to the Ninth Circuit's decision finding that an NSL letter withstood strict scrutiny. *See supra* note 124.

126. Laurent Sacharoff, *Listener Interests in Compelled Speech Cases*, 44 CAL. W. L. REV. 329 (2008).

127. *Id.* at 374–77.

128. 471 U.S. 626 (1985).

ments were unconstitutional,[129] the Court explained that the government may require mandatory disclosures of some factual information. Emphasizing that the state's "prescription has taken the form of a requirement that appellant include in his advertising *purely factual and uncontroversial* information,"[130] the Court upheld the disclosure requirement, explaining that "because [such] requirements trench much more narrowly on an advertiser's interests than do flat prohibitions on speech, warnings or disclaimers might be appropriately required in order to dissipate the possibility of *consumer confusion or deception*."[131] The logic of this opinion would not hold if the information at issue was false.

Perhaps even more telling are cases concerning mandated abortion disclosures. Courts have been particularly deferential to legislatures in terms of what disclosures they may mandate in the abortion context, notwithstanding significant doubt and resistance by the medical community.[132] And yet, even highly deferential abortion-related cases make clear that demonstrable *false* disclosure cannot be compelled. For example, in *Planned Parenthood v. Rounds*, the Eighth Circuit, sitting *en banc*, reversed an earlier panel's decision striking down a disclosure requirement that it found factually unsubstantiated.[133] But in doing so, it made clear that Planned Parenthood could have succeeded if it established that the mandated disclosure was actually "*untruthful*."[134] The Eighth Circuit simply disagreed with the panel's conclusion that the disclosure was untruthful or misleading.

Here, the compelled communication of the cryptographic keys would be unquestionably untruthful because the keys would not belong to the purported user. That, of course, is the whole point of compelling the sending of those keys. As in *Planned Parenthood v. Rounds*, where the court implied that an untruthful mandatory disclosure would have resulted in Planned Parenthood prevailing

129. *Id.* at 649.

130. *Id.* at 651 (emphasis added).

131. *Id.* (emphasis added) (cleaned up).

132. Professor Rebecca Dresser has noted this phenomenon in cataloging some examples of mandated disclosure requirements that "conflict with accepted medical knowledge." Rebecca Dresser, *From Double Standard to Double Bind: Informed Choice in Abortion Law*, 76 GEO. WASH. L. REV. 1599, 1609 (2008). She explains that this is in conflict with traditional notions of informed consent, which generally do not require physicians to warn of health risks that are not recognized by the medical community as having a causal link to a proposed procedure or medicine. *Id.* at 1618–19.

133. 686 F.3d 889, 892 (8th Cir. 2012) (en banc).

134. *Id.* at 893 (emphasis added) (cleaned up).

under strict scrutiny, an order requiring service providers to make untruthful statements is unlikely to be the least restrictive, most narrowly-tailored approach to conducting law enforcement operations.

Finally, although users are the ones ultimately targeted, the service providers are the ones whose speech is being burdened and whose reputation is at stake. Since communication service providers succeed by achieving network effects, there are naturally relatively few of them, and fewer still that feature end-to-end encryption. Thus, it is a small group of repeat players that would be routinely and repeatedly subjected to compelled speech. To the extent that strict scrutiny analysis takes into account the burden imposed on the speaker,[135] this additionally weighs against the constitutionality of an assisted MITM order because the same companies would be routinely asked to make false attestations in myriads of cases.[136]

D. Banning the Services Altogether

The above analysis, while forceful, is narrow. I argue only that, in the context of *existing* systems, the government cannot undermine the key distribution system by compelling service providers to make false attestations to their users.

An entirely separate question is whether such services may be banned altogether. As discussed in Part II.C, the Burr-Feinstein legislation introduced in the wake of the 2015 terrorist attacks in San Bernardino would have required service providers to ensure that they are able to decrypt data when writing encryption software. The

135. *See, e.g.*, Riley v. National Federation of the Blind of North Carolina, Inc., 487 U.S. 781, 798 (1988) (considering whether a compelled disclosure is "unduly burdensome" as part of the narrow tailoring factor in a strict scrutiny analysis).

136. Of course, not all compelled assistance provisions are unconstitutional. The Store Communication Act contemplates compelled assistance via subpoena, for example, *see supra* Part II.B, and one must assume that companies have been compelled to write code in response to orders issued under such subpoenas. For example, the Structured Query Language (SQL) is a programming language used to interface with many database systems, the contents of which may be the target of a subpoena. *See generally* ALAN BEAULIEU, LEARNING SQL (2d ed. 2009). What distinguishes the assisted MITM order is that the compulsion is not to write code but to *communicate* a statement (key ownership). To take the example of Apple in the San Bernardino case, the compelled order was to enable the FBI to access the unencrypted contents of the device—a device that it already had in its possession. That assistance would have required Apple to write code—which it argued was speech—but it was not the code that the government was seeking. Analogously, a subpoena for archived tax records served on a company would presumably require communications among the employees to produce the responsive records, but those incidentally necessary communications are not the real subject of the subpoena. The tax records are.

Burr-Feinstein legislation would not implicate the same constitutional issues as above, since it would not result in the government forcing a service provider to make a particular communication—it would simply make services like iMessage, WhatsApp, and Signal illegal.

I take no position on whether a law entirely banning software that features end-to-end encryption would be constitutional. As noted in Section III.A, courts have routinely found computer code to be speech for the purposes of the First Amendment. Thus, software vendors might have a colorable argument that such a ban is a content-based prior restraint on speech. On the other hand, restrictions on software (including, specifically, encryption software) have historically been implemented in terms of export controls rather than restraints on *writing* the software,[137] and one could imagine carefully written legislation that would make it essentially impossible to sell software featuring end-to-end encryption without running afoul of export regulations, even though technically *producing* such software would be legal. And there have been other proposed ways that would inhibit end-to-end encryption, including key escrow.[138] The constitutionality of these proposals is outside the scope of this Note.

I argue only that there is a sustained, and perhaps increasing, call for the government to be able to access messages sent by users over encrypted communication systems. There is at least one way for the government to do so that would require minimal technical work. But in many cases, I believe that way would not be a constitutional one.

IV.
THE RIGHTS OF THE USERS

The previous Part analyzed an assisted MITM order—a scenario in which the government compels a service provider to falsely

137. *Bernstein v. United States* was a prominent series of cases concerning export controls on encryption software in which Daniel Bernstein, a student and later professor studying cryptography, sought to publish certain papers and software code that had originally been subject to export controls. After several trips between the district court in the Northern District of California and the Ninth Circuit, the government ended up loosening the regulations and the case was dismissed as unripe. *See*, D. J. Bernstein, *Bernstein v. United States*, https://cr.yp.to/export.html [https://perma.cc/K96T-NWJA] (summarizing the controversy); 65 Fed. Reg. 2,492 (the relaxed rules). The rules currently in effect are quite broad and allow for current end-to-end encrypted products to be sold. *See, e.g.*, 15 C.F.R. § 740.17 (2018).

138. *See supra* notes 11–14 and accompanying text.

attribute government keys to the provider's users—and concluded that such an order would violate the First Amendment rights of the service provider. This Part examines the rights of the users.

Of course, while the rights of the users and service providers are separate and distinct, they are not completely isolated from one another. If a service provider is served with an assisted MITM order along with a gag order (such as under the Stored Communication Act), the service provider may be the only one in a position to assert its users' rights. A threshold question, therefore, is whether the users have any privacy rights that the service provider could assert. This Part first reviews some recent case law to show that the third-party standing doctrine forecloses that strategy. It then argues that no separate First Amendment remedy appears to be available for users and concludes by examining some of the public policy ramifications of this status quo.

A. Service Providers Cannot Assert Users' Rights on a Fourth Amendment Theory

As a general matter, federal courts strongly disfavor one party asserting another party's legal claims or rights. This is related to the rationale requiring a party to have standing and is thus rooted in Article III of the Constitution.[139] There are certain exceptions, such as "organizational standing," which allows organizations to assert certain rights on behalf of their members,[140] as well as certain "close" relationships, such as that of doctor and patient,[141] but these exceptions are few and far between. Additionally, specifically in the context of the Fourth Amendment, a separate doctrine that is also called "third-party standing" precludes the application of the exclusionary rule[142] when the "Fourth Amendment injury" was in-

139. *See generally, e.g.*, Ashwander v. Tenn. Valley Auth., 297 U.S. 288, 347 (1936) (Brandeis, J., concurring) ("The Court will not pass upon the validity of a statute upon complaint of one who fails to show that he is injured by its operation.").

140. Warth v. Seldin, 422 U.S. 490, 511 (1975).

141. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965) (finding that doctors have standing to assert their patients' privacy interests in obtaining contraception); *see also* Kowalski v. Tesmer, 543 U.S. 125, 130 (2004) (outlining requirements for this exception).

142. In the context of criminal law, the "exclusionary rule" deems inadmissible evidence that was gathered in violation of constitutional rights. *Weeks v. United States*, 232 U.S. 383 (1914), was a seminal case that announced the rule in the context of the Fourth Amendment. *Mapp v. Ohio*, 367 U.S. 643 (1961), extended the rule to state court prosecutions as well. *See generally* Richard M. Re, Note, *The Due Process Exclusionary Rule*, 127 HARV. L. REV. 1885, 1893–907 (2014) (describing commonly stated rationales for the exclusionary rule).

flicted upon someone other than the defendant.[143] For example, an individual storing his contraband at a friend's house could not avail himself of the exclusionary rule if the friend's house was searched without a warrant.[144] This is based on the view that the Fourth Amendment is a "personal right" that cannot be vicariously asserted.[145]

In the past few years, several technology companies subjected to subpoenas and warrants have filed suits against the federal government in an effort to assert their customers' interests. These companies have not been successful.

In February 2017, Judge James Robart in the Western District of Washington, held that Microsoft did not have standing to assert its customers' Fourth Amendment rights.[146] The lawsuit concerned a practice of the Department of Justice in which the Department obtained warrants for data stored in the cloud and then imposed "gag orders" under section 2705(b) of the SCA, thus preventing Microsoft from disclosing the existence of the warrants to their customers.[147] Microsoft sued on behalf of itself under the First Amendment, as well as on behalf of its customers under the Fourth Amendment. The judge denied a motion to dismiss on the First Amendment claims but dismissed the Fourth Amendment claim for lack of standing. Acknowledging the "difficult situation" the holding creates for "Microsoft's customers [who] will be practically unable to vindicate their own Fourth Amendment rights"[148] because they would never learn about the intrusion in the first place, the court nonetheless held that decades of Fourth Amendment jurisprudence commanded the result. Judge Robart noted that the "conundrum . . . is not unique to the case; it is also true of the victim of an unreasonable search in a stranger's home."[149]

---

143. *See generally* Pugh, *infra* note 159, at 987–96 (discussing third-party standing in the context of electronic data).

144. *See* Alderman v. United States, 394 U.S. 165 (1968).

145. *Id.* at 174.

146. Microsoft Corp. v. DOJ, 233 F. Supp. 3d 887, 915 (W.D. Wash. 2017).

147. *See supra* note 62 and accompanying text.

148. Microsoft Corp., 233 F. Supp. at 916.

149. *Id.* (citing *Alderman*). Note that although this is a good example of a case in which the government is not incentivized to follow the command of the Fourth Amendment, it is actually a bad analogy. The general theory for disallowing third parties to avail themselves of the exclusionary rule is that no right *of those third parties* had been violated, and in fashioning the rule, the Supreme Court did not believe the benefits of additional deterrence outweighed the costs. *See Alderman*, 394 U.S. at 174–75. In *Microsoft*, however, the data sought belonged to customers, who absolutely did have a Fourth Amendment interest in it and would be able to assert that interest had they known about it. The only reason they were not able to

An even more recent case in New York state court reached a similar result. There, the New York District Attorney's office issued 381 search warrants to Facebook in connection with an investigation into a large-scale insurance fraud conspiracy. Facebook moved to quash the warrants. The New York Supreme Court[150] denied the motion, holding that "Facebook could not assert the Fourth Amendment rights of its users."[151] Facebook appealed the order, but the Appellate Division affirmed. It held that New York civil procedure law did not provide for interlocutory review of a denial of a motion to quash a criminal warrant.[152] The New York Court of Appeals affirmed the decision as well.[153]

Facebook's unsuccessful argument rested on a distinction between warrants and subpoenas. Because the warrants at issue did not bear all the indicia of a traditional warrant (for example, unlike a typical warrant executed by law enforcement officers, the warrant here directed a third party to turn over records owned by its customers), the orders, Facebook argued, were more like subpoenas than true warrants.[154] Facebook hoped to make the distinction because under New York civil procedure law, a subpoena would be reviewable on an interlocutory appeal.[155] But it bears more general significance because the SCA specifically provides for government access to customer data by subpoena, which only requires a showing of "*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."[156]

---

do so is that they did not know about it because of the gag order. Microsoft's inability to assert its customers' Fourth Amendment rights for them is therefore rooted in traditional third-party standing doctrine, and not the special exclusionary rule doctrine from *Alderman*.

150. In New York's court system, the Supreme Court is the trial court, the Appellate Division is the intermediate appellate court, and the Court of Appeals is the court of final review.

151. *In re* 381 Search Warrants Directed to Facebook, Inc. 132 A.D.3d 11, 14 (N.Y. App. Div. 2015).

152. *Id.* at 23–24.

153. *In re* 381 Search Warrants Directed to Facebook, Inc. 78 N.E.3d 141, 142 (N.Y. 2017).

154. *See id.* at 146.

155. *Id.* ("[A] motion to quash a subpoena issued prior to the commencement of a criminal action, even if related to a criminal investigation, is 'civil by nature' . . . [and] an order resolving a motion to quash such a subpoena is a final and appealable order." (emphasis removed)).

156. 18 U.S.C. § 2703(d) (emphasis added). The Appellate Division explained that "[t]his is essentially a reasonable suspicion standard." 132 A.D.3d at 22 n.8.

A warrant, meanwhile, requires a showing of probable cause. The Appellate Division explained that by trying to argue that the warrants at issue were "subpoenas" that it could move to quash on a third-party standing theory, Facebook was trying to have its cake and eat it too:

> Facebook cannot have it both ways. On the one hand, Facebook is seeking the right to litigate pre-enforcement the constitutionality of the warrants on its customers' behalf. But neither the Constitution nor New York Criminal Procedure Law provides the targets of the warrant the right to such a pre-enforcement challenge. On the other hand, Facebook also wants the probable cause standard of warrants, while retaining the pre-execution adversary process of subpoenas. We see no basis for providing Facebook a greater right than its customers are afforded.[157]

Thus, at least the New York courts have concluded that third-party standing for orders issued under the SCA are unavailable because they should be seen as warrants subject to Fourth Amendment third-party standing doctrine. An assisted MITM order would likely face the same fate. Although the case law is highly underdeveloped, the dearth of any positive precedent renders it unlikely that service providers could successfully raise their customers' privacy rights on their behalf.[158] Until that changes,[159] a service provider would have to rely on a personal injury, such as the First Amendment theory outlined in Part III.

Because companies cannot assert the Fourth Amendment rights of their users, and because, as Judge Robart observed, users are unlikely to know they are being targeted and thus cannot assert

---

157. 132 A.D.3d at 22.

158. In 2008, the Foreign Intelligence Surveillance Court of Review found that Yahoo had standing under the Protect America Act to assert a Fourth Amendment challenge on behalf of its customers to a warrantless surveillance directive. *In re* Directives to Yahoo! Inc. Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, No. 08-01 (Fisa Ct. Rev. 2008), https://www.dni.gov/files/documents/0909/FISC%20Merits%20Opinion%2020080822.pdf [https://perma.cc/4R6A-5GHB] (approved for public release by the DNI 20140909). However, the court was careful to note that the third-party standing was specially granted by the Protect America Act. *Id.* at 10–11.

159. The *Microsoft* case has already led some academics to argue that third-party standing doctrine should be relaxed because companies are better suited than their customers for challenging warrants seeking data in the cloud. *See, e.g.*, Margot E. Kaminski, *Standing After Snowden: Lessons on Privacy Harm from National Security Litigation*, 66 DePaul L. Rev. 413, 436–38 (2017); Sarah E. Pugh, Comment, *Cloudy with a Chance of Abused Privacy Rights: Modifying Third-Party Fourth Amendment Standing Doctrine Post-*Spokeo, 66 Am. U. L. Rev. 971 (2017).

their own Fourth Amendment rights, Fourth Amendment jurisprudence is unhelpful. The next Section analyzes the user's *First* Amendment rights (again recognizing that the same obstacle of not knowing that one is the subject of an investigation would, as a practical matter, foreclose those claims anyway).

B. The First Amendment Does Not Protect Users

Putting aside the fact that users are unlikely to assert their own rights because they would not know that they are the subject of an investigation, the users whose messages are being decrypted would at least have a valid, personal Fourth Amendment claim. The users whose messages are being *forged*, however, would not have any sort of Fourth Amendment claim, since no "search" of their messages is being performed. This Section investigates whether those users could assert a First Amendment injury instead.

To make the hypothetical as friendly as possible, assume that the government is in fact forging messages, rather than simply passing them along.[160] As a threshold matter, the users will not have third-party standing to assert the service providers' First Amendment rights in a case in which the service provider simply consents to falsely attesting about a key that the government supplied. Although the keys are conceptually associated with a user (and it is in that sense that one could say they "belong" to them), they are still data legally owned by the service providers. If that service provider chooses to allow the government to falsely present a key as belonging to a user, the user (or perhaps her counterparty in a conversation) may have a breach-of-contract claim against the service provider, as well as a possible civil claim under the SCA.[161] But because, as I argue in Part III, the service provider has ample ability to assert its own First Amendment rights, a user could not stand in its shoes to assert them.[162]

160. In Figure 5 in Part I.C, the message that was being forged by the government to send to Bob as if it came from Alice was in fact the same message Alice sent. But of course, it doesn't have to be that way. For example, suppose Alice is planning a heist with Bob and messages him "take the gun, leave the cannoli." The government could intercept the encrypted message and modify it to read "take the gun and *bring* the cannoli," thus ensuring the availability of a snack when the police execute their sting operation.

161. *See* 18 U.S.C. § 2707(a) (2012).

162. *See generally* Kowalski v. Tesmer, 543 U.S. 125, 130 (2004) (explaining that a prerequisite to asserting standing of another party's rights is a showing of "a hindrance to the possessor's ability to protect his own interests" (internal quotation marks omitted)).

Thus, the First Amendment claim must be a personal one. One theoretical argument is that if the government is able to impersonate users' speech, it is in a sense compelling them to speak, thus creating a First Amendment injury. Moreover, in accordance with Professor Sacharoff's argument that compelled speech is inconsistent with the First Amendment's role in protecting listeners' interests, recipients of the government's forged messages are being "tricked" into believing they are communicating with someone they are not.[163]

To emphasize, the issue is not just that the government directs a key to be sent in the name of a particular user. The purpose of the assisted MITM attack is to allow the government to forge *arbitrary* messages from the user—that is, it allows the government to construct messages that will appear to be cryptographically signed by the user. It allows the government to do remotely, and at scale, what the police officer in *Hinton* and *Roden* was able to do by happenstance of a search incident to arrest.[164] To use a physical analogy, the scenario is not just a government official signing a letter with a target's name, but rather copying every citizen's handwriting so perfectly that the government can construct any possible missive to look as if it were written by any citizen.

It is difficult to construct an analogous fact pattern to something like this—where the government can routinely send messages and pretend that the messages are coming from somebody else, without any way for the listener to verify the identity of the sender. Cryptography is almost uniquely designed to address this problem. But one idea that comes to mind is the right of prisoners with respect to mail. Under *Thornburgh v. Abbott*,[165] prison guards may censor mail as long as the regulations guiding the censorship are "reasonably related to legitimate penological interests."[166] *Thornburgh* overruled an earlier case that invalidated a mail censorship system under something that resembled an intermediate scrutiny standard.[167] But in dicta, *Thornburgh* pointed out that the earlier case concerned itself with outgoing mail, whereas the regulation at issue in *Thornburgh* dealt with *incoming* mail. Since most censorship regulations are directed at maintaining order and security, which is far more likely to be threatened by incoming mail than outgoing

163. *See* Sacharoff, *supra* note 126.

164. *See supra* note 40.

165. 490 U.S. 401 (1989).

166. *Id.* at 413 (internal quotation omitted) (citing Turner v. Safley, 482 U.S. 78, 89 (1987)).

167. *See* Procunier v. Martinez, 416 U.S. 396, 413–14 (1974).

mail, the cases may also be distinguished on those grounds, preserving the previous holding.[168]

In any case, consider a hypothetical fact pattern in which prison officials repeatedly sent mail in the name of an inmate without his or her knowledge or consent. Recipients of the letters would have no way of knowing that the statements are not actually being made by the inmate, and the inmate would have no way of proving otherwise (at least for as long as she was incarcerated). Surely, such a program would raise First Amendment concerns—and in the context of prisons and "legitimate penological interests," it would be hard to imagine that it would pass even rational basis review. One could construe this either as the denied freedom of speech of the inmate—with the prisoner essentially being compelled to speak to the world—or, as Professor Sacharoff suggests, the injured listener interest of the recipients of the mail.[169] In any case, the injury is substantial.

And yet, notwithstanding the "listener's injury" formulation, I am hesitant to conclude that, absent an extreme situation like the prison hypothetical just described, there exists a freestanding constitutional right to what amounts to "integrity of identity." Of course, it may come up incidentally. For example, if the government repeatedly wrote messages on behalf of another user associating her with a political faction, that might violate her freedom of association. But what if the government simply posted an occasional movie review, and digitally signed it as her? Would that be illegal? It is not compelled speech, at least not as that term is usually understood. Absent specific factual circumstances, it does not necessarily interfere with her ability to access or enjoy any protected speech, nor to associate with any group. Furthermore, unlike the prison hypothetical, it does not foreclose the individual distancing herself from the comments with more speech.[170]

---

168. *See* 490 U.S. at 411–14.

169. *See* Sacharoff, *supra* note 126.

170. Another intuitive concern with the government sending messages as if they were sent by some individual is a species of privacy invasion. By "privacy," I mean a broad concept of personal integrity as sometimes applied to the "privacy" rights of bodily autonomy, such as those recognized in *Roe v. Wade* and *Lawrence v. Texas*. *See* Roe v. Wade, 410 U.S. 113, 152–54 (1973) (discussing abortion rights in the context of privacy); *see also* Lawrence v. Texas, 539 U.S. 558, 565 (2003) (discussing the case against the backdrop of Eisenstadt v. Baird, 405 U.S. 438, 453 (1972)). The privacy rights in those cases were constitutionally protected through a notion of "penumbras" of the Bill of Rights, *see Roe*, 410 U.S. at 152, but it is unclear how that translates to an injury like a MITM attack, where no restriction whatsoever is being placed on the individual.

And yet, intuitively, it feels very troubling. To be sure, we may demand a good reason for the government's behavior—otherwise it may not survive rational basis review. But such reasons are not hard to imagine. For example, the *Washington Post* has reported that the FBI has, on at least one occasion, deployed malware designed to discover a target's IP address (and thus, location) by creating a website that looked like it was operated by the Associated Press.[171] Had it been able to leverage the website's authentication system,[172] it would have been extremely difficult, if not impossible, to determine that the website was not in fact published by the media company.[173] Similarly, targets would be more likely to install software sent to them by a friend; by forging a message to look like it was coming from a known contact, the government could easily trick a target into installing malware that assists in tracking the target's location or otherwise assists in law enforcement operations. In much the same way, an assisted MITM attack would allow the government to communicate with someone who thinks they are communicating with a known associate, with full confidence of that belief founded on the cryptographic protocols implemented in their messaging services.

On the other hand, it is clear that there is *some* recognition of privacy rights for an injury of the kind discussed in this Note. For example, an individual posing as another online may be liable in tort for appropriation of likeness, a species of privacy right. *See* Bradley Kay, Note, *Extending Tort Liability to Creators of Fake Profiles on Social Networking Websites*, 10 CHI.-KENT J. INTELL. PROP. 1 (2010). The problem, however, is that the government enjoys sovereign immunity that it has not waived for privacy torts. *See* 28 U.S.C. § 2680 (2012) (listing torts for which sovereign immunity is waived under the Federal Torts Claims Act). Additionally, the Lanham Act waives sovereign immunity for both the federal government and state governments, 15 U.S.C. § 1122(a)–(b) (2012), and so individuals may have remedies for, *e.g.*, false endorsement claim. § 1125(a). Consider, for example, Bruce Springsteen suing the President for playing his music at a White House event. The Lanham Act does not reach misappropriation of likeness claims, however. *See also* Paul v. Davis, 424 U.S. 693 (1976) (holding that reputation alone is not a constitutionally protected interest).

171. Ellen Nakashima & Paul Farhi, *FBI Lured Suspect with Fake Web Page, but May Have Leveraged Media Credibility*, WASH. POST (Oct. 28, 2014), https://www.washingtonpost.com/world/national-security/fbi-lured-suspect-with-fake-web-page-but-may-have-leveraged-media-credibility/2014/10/28/e6a9ac94-5ed0-11e4-91f7-5d89b5e8c251_story.html [https://perma.cc/X982-E773].

172. Websites use authentication systems that operate on the same fundamental principles as those in end-to-end encrypted messaging systems. *See generally* GLOBALSIGN, *supra* note 30.

173. If the government successfully did that, user's web browsers would display the "green lock" or a similar graphic, making it look as if there was a secure connection to the real website. *See* MOZILLA, *supra* note 99.

Indeed, one can imagine motivations even outside the law enforcement context. Suppose, for example, that a small town was trying to prop up a local business and did so by writing glowing reviews in the names of its citizens on Yelp. That is certainly a rational basis, but intuitively, it feels troubling. And yet, I know of no constitutional reason that the town (or state or federal) government could not undertake such a program.[174]

But so what? We began this discussion by focusing on authentication. What if the government were only allowed to order the replacement of encryption keys and not verification keys? Then, the government could bypass end-to-end encryption, finally submitting it to tried-and-true Fourth Amendment doctrine. With verification keys not subject to assisted MITM orders, people's identities would remain intact.

The problem is that cryptography does not work that way. Either the government has the ability to falsely associate itself with another user's identity, or it doesn't. If it doesn't, end-to-end encryption is here to stay—recall that a verified channel is all that is needed to ensure a confidential conversation.[175] Users could use the verification keys to share *new* encryption keys to create a new, secure channel, and the government would have no way of accessing the new channel. In other words, an assisted MITM order, if it were allowed, has to be all or nothing.

---

174. As mentioned in note 171, *supra*, the users may be able to collect damages from the federal government in an analogous scenario under the Lanham Act on a false endorsement theory. But even that result is not constitutionally mandated.

This hypothetical brings to mind the plot of the Bollywood movie *Poster Boys*, in which three men discover that their likenesses were used on a poster promoting vasectomies. *See* POSTER BOYS (Sony Pictures 2017). Of course, public service announcements about family planning (in support of either birth control or procreation) are not exclusively the province of fiction. *See, e.g.*, Adam Century, *China's Colorful Family-Planning Propaganda*, THE ATLANTIC (Nov. 18, 2013), https://www.theatlantic.com/china/archive/2013/11/chinas-colorful-family-planning-propaganda/281594/ [https://perma.cc/FXB3-5TB5] (providing examples of government messaging promoting family planning in support of the one-child policy); Joshua Keating, *Rap video urges Singaporeans to get busy making babies*, FOREIGN POLICY (Aug. 8, 2012 4:23 PM), http://foreignpolicy.com/2012/08/08/rap-video-urges-singaporeans-to-get-busy-making-babies/ [https://perma.cc/7WYP-B4T6] (displaying a government-sponsored rap music video encouraging listeners to procreate). Unlike the example of the Yelp reviews, however, these examples—both real and fictional—do not need to rely on cryptography, since the likeness of any actor would be noticed visually.

175. *See supra* note 31 and accompanying text.

If the order is allowed and verification keys could be forged, society must be comfortable with the reality that the government will sometimes be able to speak in the digital voices of its citizens, without their permission or even knowledge. Courts will have to fashion tests to balance interests rarely considered together—free-floating free speech interests versus law enforcement's interest in surveillance. Is it acceptable for police officers to digitally pose as a target and express opinions in her name? If so, can it be on any topic? And for how long? This Note does not propose a resolution to this tension. But the tension is an inescapable reality of the cryptographic world we have created.

CONCLUSION

End-to-end encryption is usually discussed in the context of information privacy, and it has befuddled the government because it operates outside the rules of traditional privacy safeguards. Through Fourth Amendment doctrines and related jurisprudence, American society has struck a balance between privacy interests and law enforcement. We have almost two-and-a-half centuries' worth of experience in procedures to evaluate that tradeoff. It is no wonder that a sudden wrench in that history feels so disruptive.

But "end-to-end encryption" is little more than a marketing term. The sort of confidentiality it promises are consequences of basic mathematical facts, whose efficacy is based not on any sort of privacy concerns but on the knowledge that individuals know whom they're speaking with. That is the foundation we must be willing to disturb if we decide that end-to-end encryption is too dangerous to allow. As it stands, we have entrusted third parties to accurately connect us to our counterparties, and for as long as that trust is respected, traditional First Amendment doctrine protects those parties from conscription into government surveillance. If those parties do not object to an assistance order, however, citizens are without recourse. There is no question that the Framers did not anticipate this conundrum when they were drafting the Bill of Rights. Now that the reality is upon us, however, we should determine if we should allow it. If it is a step we are willing to take, we ought to take it deliberately.