Apple’s “Communication Safety” Feature for Child Users: Implications for Law Enforcement’s Ability to Compel iMessage Decryption

Nicholas A. Weigel*

STAN. TECH. L. REV. 210 (2022)

ABSTRACT

In August 2021, Apple announced plans to add several features to its iPhone operating system (iOS) to help prevent the possession and dissemination of child sex abuse material (CSAM). Among the proposals was a feature to be deployed on child iMessage accounts that would use a machine learning algorithm to scan all incoming and outgoing photos in a child’s messages for nudity. This feature would come to be branded “Communication Safety” and was implemented in the United States as part of a routine iOS update in December 2021.

The public reaction to Communication Safety has been relatively subdued, in stark contrast to the outcry from privacy advocates and information security experts in response to Apple’s proposed “client-side scanning” feature. This Note argues, however, that despite the relatively muted reaction to its announcement, Communication Safety also presents a meaningful risk to user privacy and security, constituting the early architecture of a backdoor into iMessage’s encryption—one that could theoretically be expanded with only a few technical modifications.

This Note discusses how U.S. law enforcement could attempt to use existing legal authorities to compel Apple to modify Communication Safety to search or surveil a suspect’s encrypted messages that otherwise would be beyond the government’s reach. While it is uncertain whether a court would ultimately issue such an order, Apple’s introduction of Communication Safety strengthens the government’s legal arguments in its longstanding effort to compel the company to assist with decrypting its users’ communications.
TABLE OF CONTENTS
I. INTRODUCTION .............................................................................................................. 211
II. “GOING DARK,” iMESSAGE ENCRYPTION, AND COMMUNICATION SAFETY .......... 214
III. ACCESSING STORED iMESSAGES PURSUANT TO A RULE 41 SEARCH WARRANT .... 218
   A. The Stored Communications Act ........................................................................... 218
   B. The All Writs Act .................................................................................................. 219
       2. Apple v. FBI..................................................................................................... 221
          i. All Writs Act Arguments .......................................................................... 223
          ii. CALEA Arguments ................................................................................. 226
          iii. Outcome ................................................................................................. 228
   C. Application to Communication Safety Scenario .................................................... 230
IV. REAL-TIME INTERCEPTION OF iMESSAGES PURSUANT TO A WIRETAP ACT OR FISA ORDER ................................................................. 234
   A. Car Eavesdropping Case: Minimum of Interference Limitation ................. 236
   B. United States v. Lavabit: Furnishment of Information and Assistance 237
   C. Facebook Messenger Case: A Broader View of “Minimum of Interference?” .................................................. 240
   D. Application to Communication Safety Scenario .................................................. 242
V. CONCLUSION .................................................................................................................. 244

I. INTRODUCTION

In August 2021, Apple announced plans to add several features to its iPhone operating system (iOS) to help prevent the possession and dissemination of child sex abuse material (CSAM), an urgent and growing problem. Among the proposals was a “client-side scanning” feature that would work by comparing the digital fingerprints (“hashes”) of photos saved to a user’s iCloud account against the hashes in a database of known child pornography images. If a certain number of photos in the user’s account matched those in the database, Apple would be alerted, initiating a human review of the photos. If the photos were verified to contain CSAM, Apple would report the user to the National Center for Missing & Exploited Children.

* J.D. Candidate, Harvard Law School, Class of 2023. Many thanks to Jack Goldsmith for his helpful comments and guidance, and to Jim Baker for helping me develop the initial idea for this Note. Thank you also to the editors of the Stanford Technology Law Review, including Katherine Viti, Erin Sifre, Mitchell Perry, Haley Chow, and Jun Hong Tan, for their assistance. Any errors are mine alone.

2 Expanded Protections for Children, supra note 1.
3 Id.
(NCMEC), which would then alert law enforcement. This feature was described as a “client-side scanning” system because the comparison function would occur on the user’s device (“client-side”), not on Apple’s servers (“server-side”), an arrangement some consider to be more protective of user privacy. Nevertheless, Apple’s proposal was immediately met with fierce opposition from privacy advocates and information security experts alike, who argued that the system opened the door to broader government surveillance and threatened to undermine Apple’s encryption protocols, which help protect the privacy and security of users’ data and communications. Apple responded by indefinitely delaying implementation of the feature.

More subdued was the reaction to another child safety tool that Apple announced—what would come to be branded “Communication Safety.” As proposed, this feature would be deployed on child iMessage accounts and, if engaged by a parent, would use a machine learning algorithm to scan all incoming photos in a child’s messages for nudity. If nudity was detected, the photo would be blurred and a warning would appear alerting the child to the potentially graphic content. All outgoing photos sent by the child would also be scanned for nudity. The idea was to add friction to the transmission of CSAM by providing child users with warnings and resources should an adult try to coerce them into sending or accepting nude photos via the Messages app. After making a small tweak to the feature, Apple officially rolled out Communication Safety in the United States as part of a routine software update.

4 Id.
5 See Riana Pfefferkorn, Client-Side Scanning and Winnie-The-Pooh Redux (Plus Some Thoughts on Zoom), CTR. FOR INTERNET & SOC’Y (May 11, 2020), https://perma.cc/LJF6-ED45. Some experts consider client-side scanning to be less protective of privacy than server-side scanning. See, e.g., Ben Thompson, Apple’s Mistake, STRATECHERY (Aug. 9, 2021), https://perma.cc/RHG2-8A2D (“[I]nstead of adding CSAM-scanning to iCloud Photos in the cloud that they own and operate, Apple is compromising the phone that you and I own and operate, without any of us having a say in the matter.”).
9 About Communication Safety in Messages, supra note 8.
10 Id.
11 Id.
(iOS 15.2) in mid-December 2021 and will soon introduce the feature in the United Kingdom, Canada, Australia, and New Zealand.

While most commentators focused their attention and outrage on Apple’s proposed client-side scanning tool, others pointed out that with the introduction of Communication Safety, the content of some children’s messages would now be monitored by a proprietary Apple algorithm. Although the feature does not grant Apple itself access to the content of child users’ messages—technically preserving iMessage’s encryption—some experts have argued that the feature is only a few steps away from giving third parties, including governments, a backdoor into any user’s communications, which could be used to scan for any type of content.

In light of these concerns, this Note argues that despite the relatively muted reaction to its announcement compared to Apple’s client-side scanning tool, Communication Safety also presents a meaningful risk to user privacy and security, constituting the early architecture of a backdoor into iMessage’s encryption—one that could theoretically be expanded into a full-scale exploit with only a few technical modifications. The algorithm that scans child users’ messages for nudity could potentially be repurposed at the request of.

12 About iOS 15 Updates, APPLE, https://perma.cc/V68S-LLSB. Originally, the child’s parent would automatically be notified if nudity was detected in an incoming or outgoing photo message. However, after child safety experts criticized this aspect of the feature, it was abandoned and replaced with a feature whereby the child can voluntarily notify a parent. See Christopher Parsons, Apple’s Monitoring of Children’s Communications Content Puts Children and Adults at Risk, TECH., THOUGHTS, & TRINKETS (Aug. 6, 2021), https://perma.cc/2VWJ-YFPN; Jason Kelley, Apple’s Plan to Scan Photos in Messages Turns Young People Into Privacy Pawns, ELEC. FRONTIER FOUND. (Aug. 27, 2021), https://perma.cc/KH8T-FGHV; Kendra Albert (@KendraSerra), TWITTER (Aug. 5, 2021, 3:28 PM), https://twitter.com/KendraSerra/status/1423365222841135114, https://perma.cc/N354-Z26P (“These ‘child protection’ features are going to get queer kids kicked out of their homes, beaten, or worse.”).


15 APPLE, EXPANDED PROTECTIONS FOR CHILDREN: FREQUENTLY ASKED QUESTIONS v.1.1 3 (2021), https://perma.cc/82G8-YENS.

governments to access and monitor the decrypted content of any iMessage user’s communications. Apple has issued assurances that it would “not accede to any government’s request to expand” its CSAM tools. But as this Note discusses, U.S. law enforcement could attempt to use existing legal authorities to compel Apple to modify its Communication Safety feature to search or surveil a suspect’s messages that otherwise would be beyond the government’s reach. While it is uncertain whether a court would ultimately issue such an order, Apple’s introduction of Communication Safety strengthens the government’s legal arguments in its longstanding effort to compel the company to assist with decrypting its users’ communications.

This Note begins by explaining how iMessage’s encryption currently frustrates law enforcement’s efforts to obtain the content of suspects’ communications and how Communication Safety might provide a backdoor solution to this problem. Part III then explores how U.S. law enforcement could potentially utilize a Rule 41 search warrant and the All Writs Act to compel Apple to repurpose Communication Safety to circumvent iMessage’s encryption. Looking back at the standoff between Apple and the FBI in 2016, where the government attempted to leverage the All Writs Act to compel Apple to help unlock the iPhone of the perpetrator of the San Bernardino terrorist attack, Apple’s introduction of Communication Safety strengthens the government’s legal arguments compared to that case. Part IV explores how the government could alternatively compel Apple’s assistance under the Wiretap Act or Foreign Intelligence Surveillance Act (FISA) to surveil a suspect’s encrypted iMessages in real time. The Note concludes by discussing proposed U.S. legislation to disincentivize companies from deploying encryption and to explicitly provide the government with the authority to compel decryption.

II. “GOING DARK,” iMESSAGE ENCRYPTION, AND COMMUNICATION SAFETY

Encrypted communications have long presented an obstacle to law enforcement’s ability to gather valuable evidence in criminal investigations—often described as the “Going Dark” problem. There exists a wide range of

---

17 Apple, supra note 15.
18 See Going Dark: Lawful Electronic Surveillance in the Era of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Jud. Comm., 112th Cong. (2011) (statement of Valerie Caproni, General Counsel, FBI), https://perma.cc/Y5KZ-Z4QH (“[O]n a regular basis, the government is unable to obtain communications and related data, even when authorized by a court to do so. We call this capabilities gap the ‘Going Dark’
views on this issue, with law enforcement officials at one end of the spectrum, arguing for the need to preserve access for investigators, and privacy advocates at the opposite end, extolling the benefits of encryption or arguing that the “Going Dark” problem is overstated.  

In law enforcement’s eyes, the “Going Dark” problem has only grown more acute as encryption has become more ubiquitous among popular communications platforms. In 2011, Apple introduced iMessage, the default messaging service for the world’s now one billion iPhone users, which it claimed featured “secure end-to-end encryption.” As cybersecurity journalist Nicole Perlroth explains:

End-to-end encryption scrambles messages in such a way that they can be deciphered only by the sender and the intended recipient. As the label implies, end-to-end encryption takes place on either end of a

problem.”); James B. Comey, Director, FBI, Remarks at the Brookings Institution, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014), https://perma.cc/X55L-KYDC (“We call it ‘Going Dark,’ and what it means is this: Those charged with protecting our people aren’t always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority.”); Kristin Finklea, Cong. Rsch. Serv., R44481, Encyption and the “Going Dark” Debate 1 (2017).

See, e.g., William P. Barr, Attorney General, Keynote Address at the International Conference on Cyber Security (Jul. 23, 2019), https://perma.cc/TCA-MPXH (arguing that encryption creates “law-free zones’ insulated from legitimate scrutiny”); Comey, supra note 18 (“T]he notion that the marketplace could create something that would prevent that closet from ever being opened, even with a properly obtained court order, makes no sense to me.”); Andrew Crocker & Nate Cardozo, New National Academy of Sciences Report on Encryption Asks the Wrong Questions, Elec. Frontier Found. (Feb. 16, 2018), https://perma.cc/HT24-RPBK (“T]he adoption of encryption by default is one of the most positive developments in technology policy in recent years because it permits regular people to keep their data confidential from eavesdroppers, thieves, abusers, criminals, and repressive regimes around the world.”); David Ruiz, Congressmembers Raise Doubts About the “Going Dark” Problem, Elec. Frontier Found. (Apr. 17, 2018), https://perma.cc/6YYY-P6RF (discussing a March 2018 Department of Justice Office of the Inspector General report raising questions about the extent of the “Going Dark” problem); Jim Baker, Rethinking Encryption, Lawfare (Oct. 22, 2019), https://perma.cc/BKD7-E6T9 (former FBI General Counsel arguing that the cybersecurity benefits of encryption outweigh the investigative challenges it creates for law enforcement).

See Susan Hennessey, Lawful Hacking and the Case for a Strategic Approach to “Going Dark”, Brookings Inst. (Oct. 7, 2016), https://perma.cc/E67K-UEFB (“The problem’s scale has increased dramatically over the past few years, as a number of major communications providers have taken steps towards offering end-to-end encrypted messaging and sophisticated device encryption broadly and by default.”).

Jacob Kastrenakes, Apple Says There Are Now Over 1 Billion Active iPhones, Verge (Jan. 27, 2021), https://perma.cc/9S9E-X55L.

communication. A message is encrypted on a sender’s device, sent to
the recipient’s device in an unreadable format, then decoded for the
recipient. . . . End-to-end encryption ensures that no one can
eavesdrop on the contents of a message while it is in transit. It forces
spies or snoops to go directly to the sender or recipient to read the
content of the encrypted message. 23

In the years since Apple’s announcement of iMessage and its
purported end-to-end encryption, however, researchers and law enforcement
authorities have discovered an important caveat: iMessages that are backed up
to a user’s iCloud account can be decrypted by Apple, often at the government’s
request. 24 When an iPhone user has enabled “iCloud Backup” or “Messages on
iCloud,” Apple can access the key required to decrypt the user’s messages. 25
The government therefore routinely serves Apple with court orders to turn over
the messages stored in suspects’ iCloud accounts. In many cases, this is
sufficient to satisfy the government’s investigatory needs, though it is
important to note that the iCloud loophole does nothing to resolve the
government’s persistent inability to intercept a suspect’s iMessages in real
time. 26 Furthermore, even in some cases where the government is only seeking
access to stored iMessages, a suspect will have turned backups off, leaving the
government with no means to circumvent iMessage’s encryption protocol and
access the suspect’s messages. This was the case of the terrorist who carried
out a mass shooting in San Bernardino, California in December 2015, which set

23 Nicole Perlioth, What Is End-to-End Encryption? Another Bull’s-Eye on Big Tech, N.Y. TIMES
(Nov. 19, 2019), https://perma.cc/JRY4-3YBX.
24 Maximilian Zinkus ET AL., DATA SECURITY ON MOBILE DEVICES: CURRENT STATE OF THE ART, OPEN
PROBLEMS, AND PROPOSED SOLUTIONS §§ 1.1.1, 3.1, Figure 3.6 (May 27, 2021),
https://perma.cc/2A85-CK34 (“Apple’s ‘Messages in iCloud’ feature advertises the use of an
Apple-inaccessible ‘end-to-end’ encrypted container . . . . However, activation of iCloud
Backup in tandem causes the decryption key for this container to be uploaded to Apple’s
servers in a form that Apple (and potential attackers, or law enforcement) can access.”);
William Gallagher, What Apple Surrenders to Law Enforcement When Issued a Subpoena,
APPLEINSIDER (Jan. 21, 2020), https://perma.cc/KM3M-ALFG; Thomas Brewster, When
iMessages Aren’t Private: Government Raids Apple iCloud In A Dark Web Drug Investigation,
FORBES (Feb. 15, 2021, 9:55 AM EST), https://perma.cc/6CMX-5GT3; see also CloudKit End-to-
End Encryption, APPLE (Feb. 18, 2021), https://perma.cc/8EPD-HGV9; APPLE, LEGAL PROCESS
GUIDELINES: GOVERNMENT & LAW WITHIN THE UNITED STATES § 3.1, https://perma.cc/BW9F-YUWK.
25 Gallagher, supra note 24.
26 See Riana Pfefferkorn, We Now Know What Information the FBI Can Obtain from Encrypted
FBI document); Declan McCullagh & Jennifer Van Grove, Apple’s iMessage Encryption Trips
up Feds’ Surveillance, CNET (Apr. 4, 2013, 4:00 AM PT), https://perma.cc/J44Z-JVYX (citing a
DEA document).
off a high-stakes legal dispute between Apple and the FBI, discussed in greater
detail in Part III.B.2.  

Communication Safety could offer a solution to this “Going Dark”
problem. As previously discussed, when the Communication Safety feature is
engaged, before a child user sends or receives an image in iMessage, a machine
learning algorithm scans the image—in its decrypted form—for nudity. If the
algorithm detects nudity, a warning appears alerting the child to the potentially
graphic content, which the child remains free to disregard. The warning also
contains an option to alert a parent. An earlier proposal would have
automatically notified a parent if the child chose to view or send the image, but
that feature was scrapped following public criticism. While the
Communication Safety feature is designed to examine images (and only for
nudity), the algorithm could theoretically be modified to scan for and flag other
types of content, including text, such as specific words or phrases. Furthermore, although the feature is currently only available for child
accounts—and is not turned on by default—there is little preventing Apple from
surreptitiously enabling the feature on other accounts. As India McKinney &
Erica Portnoy of the Electronic Frontier Foundation explain:

All it would take to widen the narrow backdoor that Apple is building
is an expansion of the machine learning parameters to look for
additional types of content, or a tweak of the configuration flags to
scan, not just children’s, but anyone’s accounts. That’s not a slippery
slope; that’s a fully built system just waiting for external pressure to
make the slightest change.

The Communication Safety feature could then conceivably be modified
further to automatically notify Apple of an algorithmic match and share with
the company the flagged content, whether an image or a string of text. Apple
could then be forced to share the content with government authorities. A

27 See infra text accompanying notes 63-126.
28 See supra text accompanying notes 8-11.
29 About Communication Safety in Messages, supra note 8.
30 Id.
31 Id.
32 See Parsons, supra note 12; Kelley, supra note 12; Albert, supra note 12.
33 See Cox, supra note 14 (quoting Matthew Green as suggesting Apple could use
Communication Safety for other purposes).
34 McKinney & Portnoy, supra note 16.
repurposed Communication Safety feature therefore could serve as a means to circumvent iMessage’s encryption.

III. ACCESSING STORED iMESSAGES PURSUANT TO A RULE 41 SEARCH WARRANT

Consider the following scenario: law enforcement is investigating a suspect known to use iMessage to communicate. The suspect has turned off iCloud backup, meaning his iMessages are stored only on his device and Apple does not possess the key necessary to decrypt them.35 The government, upon demonstrating probable cause that the suspect’s communications contain evidence of a crime, obtains a warrant under Rule 41(c) of the Federal Rules of Criminal Procedure to search the suspect’s iMessage account.36 Until recently, the government’s investigation would hit a wall at this point, as Apple had no means of accessing the content of the suspect’s encrypted iMessages. But this may no longer be the case now that Apple has rolled out Communication Safety. As discussed in Part II, the Communication Safety feature can conceivably be adapted to scan any user’s messages for other types of content, such as specific words or phrases, and, if detected, share that content with Apple and, in turn, law enforcement.37 Recognizing this, law enforcement attempts to take advantage of this theoretical backdoor into iMessage. Drawing on existing legal authorities, the government seeks to obtain a court order to compel Apple to make such modifications to its Communication Safety feature to effectuate a duly issued warrant to search a suspect’s iMessage account. This Part discusses the authorities that might enable such compelled technical assistance, most notably the All Writs Act.

A. The Stored Communications Act

The Stored Communications Act (SCA) does not provide the government with the authority to compel Apple’s assistance in this scenario. At first glance, Apple appears to fall within the SCA’s required disclosure provision, under which the government may compel a provider of an electronic communication service to disclose the contents of communications that are “in

35 See Gallagher, supra note 24.
36 See United States v. N.Y. Tel. Co., 434 U.S. 159, 169 (1977) (citing Katz v. United States, 389 U.S. 347, 354-56 (1967)) (“Rule 41 is not limited to tangible items but is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause.”).
37 See supra text accompanying notes 33-34.
electronic storage.” However, the Eleventh Circuit in 2003 held that the SCA’s provisions do not extend to end-user devices. The Fifth Circuit in a civil case in 2012 specifically held that messages stored solely on an individual’s cell phone (and not on a central server) are not “in electronic storage” under the statute. Other circuits have held similarly. Therefore, the SCA does not provide a statutory basis for the government to compel Apple to help provide the content of iMessages not stored on its servers.

B. The All Writs Act

The government could have greater success leveraging the All Writs Act to compel Apple’s assistance. Originally enacted in 1789, the All Writs Act empowers a court to “issue all writs necessary or appropriate” to exercise its jurisdiction. As the Supreme Court has explained, “The All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute.” In other words, the All Writs Act is a “gap filler” provision. Relevant to the scenario at hand, courts have held that the Act “permits [a] district court, in aid of a valid warrant, to order a third party to provide nonburdensome technical assistance to law enforcement officers.” Therefore, in order to effectuate a duly issued Rule 41 search warrant, a court could potentially invoke the All Writs Act to order Apple to provide the government with the technical assistance necessary to access the decrypted content of a suspect’s iMessages. This subsection discusses the leading cases adjudicating the scope of the All Writs Act, United States v. New York Telephone Company and Apple v. FBI (otherwise known as the San Bernardino iPhone case). Part III.C then applies the arguments and rulings in these cases to the hypothetical Communication Safety scenario.

---

39 United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003).
40 Garcia v. City of Laredo, 702 F.3d 788, 793 (5th Cir. 2012).
42 1 Stat. 73 § 14 (1789).
46 Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283, 1289 (9th Cir. 1979) (citing United States v. N.Y. Tel. Co., 434 U.S. 159, 172 (1977)).
1.  *United States v. New York Telephone Company*

In 1977, the Supreme Court rejected a challenge by a telephone company seeking to invalidate a district court order compelling the company to furnish law enforcement with the technical assistance necessary to install two pen registers as part of an investigation into illegal gambling.\(^{47}\) While Congress had passed the Wiretap Act\(^ {48}\) in 1968 to govern surveillance of the content of communications, no statute at the time of the case specifically addressed the installation and operation of pen registers, which capture the numbers a phone dials or, in modern times, that a user messages.\(^ {49}\) The Court ultimately held that the district court’s order was a valid exercise of its authority under Rule 41 of the Federal Rules of Criminal Procedure and the All Writs Act.\(^ {50}\) The Court stressed, however, that a court’s authority under the All Writs Act is not without limits.\(^ {51}\) The Court declared that “[u]nreasonable burdens may not be imposed” and laid down three specific requirements.\(^ {52}\) First, the third party whose assistance is to be compelled must not be “so far removed from the underlying controversy.”\(^ {53}\) Second, the order must not be unduly “burdensome” to the third party.\(^ {54}\) Finally, the third party’s assistance must be “essential to the fulfillment” of law enforcement’s objectives.\(^ {55}\)

The Court determined that, because all three requirements were satisfied, the requested assistance was not unreasonable. First, the telephone company was sufficiently connected to the investigation because there was probable cause to believe its facilities were being used for unlawful activity.\(^ {56}\) The Court also noted that the company was a “highly regulated public utility with a duty to serve the public.”\(^ {57}\) Second, the assistance would not be “burdensome” because it would require “minimal effort” from the company, it would not disrupt its operations, and the company would be compensated by

---


\(^{49}\) 434 U.S. at 166-67. In 1986, as part of the Electronic Communications Privacy Act (ECPA), Congress passed the Pen Register and Trap and Trace Act, codified at 18 U.S.C. §§ 3121-3127.

\(^{50}\) 434 U.S. at 170, 172.

\(^{51}\) Id. at 172.

\(^{52}\) Id.

\(^{53}\) Id. at 174.

\(^{54}\) Id. at 175.

\(^{55}\) Id.

\(^{56}\) Id. at 174.

\(^{57}\) Id.
the government for its efforts.\textsuperscript{58} Finally, the Court determined that there was no alternative way for the FBI to covertly install the pen registers without the company’s assistance.\textsuperscript{59}

The New York Telephone Co. framework has remained the governing test for All Writs Act orders. In the years since the Supreme Court’s decision, courts have issued All Writs Act orders requiring a defendant to provide law enforcement with the password necessary to decrypt files on his own computer,\textsuperscript{60} Citibank to provide a defendant’s credit card records,\textsuperscript{61} and a landlord to provide security camera tapes,\textsuperscript{62} among other examples of compelled assistance.

2. \textit{Apple v. FBI}

On December 2, 2015, Syed Rizwan Farook, along with his wife, Tashfeen Malik, carried out a mass shooting attack in San Bernardino, California, killing fourteen people and injuring twenty-two others.\textsuperscript{63} The FBI later uncovered evidence that the couple was inspired by ISIS.\textsuperscript{64} As part of its investigation into the attack, the FBI obtained a warrant to search Farook’s iCloud account (Farook used an iPhone) and thereby access his backed-up iMessages in decrypted form.\textsuperscript{65} However, the most recent iCloud backup from Farook’s iPhone occurred on October 19, meaning approximately six weeks of potentially relevant iMessages resided solely on his iPhone.\textsuperscript{66} The FBI obtained a warrant to search Farook’s iPhone, but soon discovered the device was “locked” by a passcode, which the FBI did not possess.\textsuperscript{67} Complicating matters further, the device was running the ninth iteration of Apple’s iPhone operating system (iOS 9), which included an auto-erase function that would permanently and irreversibly encrypt the device’s contents after ten failed passcode

\textsuperscript{58} Id. at 175.
\textsuperscript{59} Id.
\textsuperscript{60} United States v. Fricosu, 841 F. Supp. 2d 1232, 1238 (D. Colo. 2012).
\textsuperscript{63} Government’s Ex Parte Application for Order Compelling Apple Inc. to Assist Agents in Search at 1, \textit{In re the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451M} (C.D. Cal. Feb. 16, 2016), ECF No. 18 [hereinafter Government’s San Bernardino Application].
\textsuperscript{64} Id. at 2.
\textsuperscript{65} Id. at 16-17.
\textsuperscript{66} Id. at 17.
\textsuperscript{67} Id. at 3.
In addition, the operating system had a time delay feature that prevented anyone from inputting a passcode for an increasing amount of time after each failed attempt.

To overcome these challenges, the FBI sought a court order pursuant to the All Writs Act to compel Apple to provide technical assistance to help “unlock” the device. Specifically, the FBI requested that Apple create software that could be loaded onto Farook’s device and would (1) bypass or disable the auto-erase feature to allow unlimited passcode attempts, (2) limit the time delay after a failed attempt, and (3) enable the FBI to input passcodes electronically rather than manually. Magistrate Judge Sheri Pym issued the requested order.

In the years leading up to the dispute, Apple had routinely complied with court orders under the All Writs Act directing the company to assist law enforcement with extracting data, including iMessages, from locked iPhones.

As Apple explained, however, prior instances of assistance involved devices running iOS 7 or earlier, which did not have the same passcode-protection features that iOS 8 and subsequent iterations did. Faced with a court order compelling the company to help unlock Farook’s iPhone running iOS 9, Apple refused and moved to vacate the order.

At the same time as the San Bernardino case was unfolding, Apple and the FBI were also engaged in a legal standoff in a drug trafficking case in the Eastern District of New York (EDNY), where the FBI was similarly seeking Apple’s

---

68 Id. at 3, 5.
69 Id. at 3.
70 Id. at 7-9.
71 Id.
72 Order Compelling Apple, Inc. to Assist Agents in Search, In re the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451M (C.D. Cal. Feb. 16, 2016), ECF No. 19 [hereinafter San Bernardino Order].
74 Apple Inc.’s Memorandum of Law in Response to the Government’s Brief at 5, In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by the Court, No. 1:15-MC-01902 (E.D.N.Y. Oct. 8, 2015), ECF No. 40 [hereinafter Apple’s EDNY Brief].
75 Apple Inc.’s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, In re the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 5:16-CM-00010 (C.D. Cal. Feb. 19, 2016), ECF No. 16 [hereinafter Apple’s San Bernardino Brief].
assistance unlocking a defendant’s iPhone. Whereas in the San Bernardino case the government successfully obtained an initial court order compelling Apple’s assistance, in the EDNY case, Magistrate Judge James Orenstein viewed the government’s application more skeptically and rejected it, which the government then appealed. The arguments advanced by Apple and the FBI in the ensuing litigation were substantively the same as in the San Bernardino case.

i. All Writs Act Arguments

In its motion to compel Apple’s assistance, the government argued that the court was well within its authority under the All Writs Act to compel Apple to help unlock Farook’s device. The government noted that no statute addressed the specific situation at hand: extracting data “at rest” (as opposed to data “in motion”) from a passcode-locked mobile phone. Therefore, the court was empowered to exercise its residual authority under the All Writs Act to effectuate its duly issued search warrant.

The government argued that all three factors from New York Telephone Co. were satisfied. First, Apple was not “so far removed from the underlying controversy that its assistance could not be permissibly compelled,” because Apple was the manufacturer of the device and its software, which were used in the furtherance of criminal activity. While the government acknowledged that New York Telephone Co. involved a “highly regulated public utility,” courts had previously issued All Writs Act orders to private entities as well. Second, the government argued that Apple’s assistance was “essential to ensuring that the

76 Memorandum and Order, In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by the Court, No. 1:15-MC-01902 (E.D.N.Y. Oct. 8, 2015), ECF No. 2 [hereinafter EDNY Order I]. The iPhone at issue in the EDNY case was running iOS 7, but Apple nevertheless objected to the FBI’s request for assistance. Apple’s EDNY Brief, supra note 74, at 5.
77 See Order Denying Motion to Compel, In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by the Court, No. 1:15-MC-01902 (E.D.N.Y. Oct. 8, 2015), ECF No. 29 [hereinafter EDNY Order II].
78 Government’s Motion to Compel Apple Inc. to Comply at 7-18, In re the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 5:16-CM-00010 (C.D. Cal. Feb. 19, 2016), ECF No. 1 [hereinafter Government’s San Bernardino Brief].
79 Id. at 22.
80 Id.
81 Id. at 10-12.
82 Id. at 11-12.
government is able to execute the warrant.” 83 Without Apple’s assistance disabling the specified iPhone security features, the government could not attempt to access the device without risking the permanent destruction of potential evidence. 84 The government asserted that both Apple and the FBI could not identify any alternative, feasible methods of gaining access to Farook’s iMessages sent and received between the device’s last iCloud backup and the attack. 85 Finally, the government argued that the requested assistance would not impose an “unreasonable burden” on Apple, as “writing software code in [a] discrete and limited manner” poses no difficulty “for a company that writes software code as part of its regular business.” 86 At no point did Apple dispute that it did “not have the technical ability to comply” or contend that rendering the requested assistance would be “unreasonably challenging.” 87 Furthermore, the order called for software that would be “tailored for and limited to” Farook’s device, not a “master key.” 88 The court’s order to compel would “not mean the end of privacy,” the government maintained. 89

Apple disagreed that the New York Telephone Co. factors were met. First, Apple argued that its connection to the investigation was “too attenuated.” 90 Apple had “merely . . . placed a good into the stream of commerce,” and to compel Apple to assist with the investigation would “eviscerate” any limiting factor to a company’s responsibility for the behavior of its customers under the law. 91 Apple also pointed out that the company was not a “highly regulated public utility with a duty to serve the public” with “no substantial interest in not providing assistance.” 92 To the contrary, Apple had stressed to its customers that “encryption is crucial to protect the security and privacy interests of citizens who use and store their most personal data on their iPhones.” 93 Second, Apple argued that its assistance was not “imperative” to effectuate the warrant. 94 The FBI had not “exhausted all other avenues for

83 Id. at 16.
84 Id. at 17.
85 Id.
86 Id. at 13.
87 Id. at 14.
88 Id. at 15.
89 Id.
90 Apple’s San Bernardino Brief, supra note 75, at 20.
91 Id. at 22-23.
92 Id. at 21-22 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 174 (1977)).
93 Id. at 22.
94 Id. at 29.
recovering [Farook’s iMessages].” Lastly, Apple claimed that the court’s order imposed on the company an “unprecedented and oppressive burden.” Apple claimed that creating the requested software would entail substantial engineering hours. Doing so would also set a precedent that would result in “tens of thousands” of similar requests by federal and state prosecutors, forcing Apple to create an entirely new “hacking” department. “Nothing in federal law allows the courts, at the request of prosecutors, to coercively deputize Apple and other companies to serve as a permanent arm of the government’s forensics lab,” the company argued. It would also not be in the public interest to compel Apple to render the requested assistance because the software capable of bypassing iOS passcode-protection features could fall into the hands of criminals and hackers, threatening the security of any iPhone.

The government accused Apple of refusing to comply with the court’s order due to “concern for its business model and public brand marketing strategy.” “The burden associated with compliance with legal process is measured based on the direct costs of compliance, not on other more general considerations about reputations or the ramifications of compliance,” the government argued. “Impinging on Apple’s marketing of its products as search-warrant-proof is not an undue burden,” the government later argued in its reply to Apple’s motion. The government also disputed Apple’s claim that the requested software could fall into the wrong hands. The government pointed out that Apple had successfully guarded other security-compromising

---

95 id.
96 id. at 23.
97 id. (“Although it is difficult to estimate, because it has never been done before, the design, creation, validation, and deployment of the software likely would necessitate six to ten Apple engineers and employees dedicating a very substantial portion of their time for a minimum of two weeks, and likely as many as four weeks.”).
98 id. at 24, 26.
99 id. at 26-27.
100 id. at 25.
101 Government’s San Bernardino Brief, supra note 78, at 2-3.
102 id. at 16.
103 Government’s Reply in Support of Motion to Compel and Opposition to Apple Inc.’s Motion to Vacate Order at 30, In re the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KG0203, No. 5:16-CM-00010 (C.D. Cal. Feb. 19, 2016), ECF No. 149 [hereinafter Government’s San Bernardino Reply Brief].
104 id. at 24.
software in its possession and that the requested code would only work on Farook’s device.105

**ii. CALEA Arguments**

Apple also argued that the court lacked authority to issue an All Writs Act order altogether because another statute—the Communications Assistance for Law Enforcement Act (CALEA)106—controlled and implicitly, if not explicitly, exempted entities like Apple from being compelled to provide technical assistance of the kind the FBI requested.107

Enacted in 1994, the primary purpose of CALEA was purportedly to “preserve the government’s ability, pursuant to court order or other lawful authorization, to intercept communications” as telecommunications carriers transitioned from analog equipment to digital systems.108 Digitalization of telecommunications infrastructure had begun to impede law enforcement’s ability to install and operate wiretaps, so Congress stepped in to require telecommunications carriers to “ensure that [their] equipment, facilities, or services . . . are capable of . . . enabling the government . . . to intercept . . . all wire and electronic communications carried by the carrier.”109 Congress defined “telecommunications carrier” as any “entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire” (i.e., a traditional phone service provider like Verizon or AT&T today).110 Importantly, Congress exempted “information services,” which by definition included “electronic messaging services,” from the statute’s requirements.111 This exemption was an effort to “avoid impeding the development of new communications services and technologies.”112

Apple pointed to that exemption to argue that Congress had specifically declined to require non-telecommunications carriers to “create

---

105 Id. at 24-25.
107 See Apple Inc.’s Reply to Government’s Opposition to Apple Inc.’s Motion to Vacate Order at 7-13, In re the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. S:16-CM-00010 (C.D. Cal. Feb. 19, 2016), ECF No. 177 [hereinafter Apple’s San Bernardino Reply Brief].
systems to assist law enforcement in its investigatory efforts,” such as the software the FBI was seeking. Therefore, Apple contended, CALEA “forbids” the government from compelling the company to unlock Farook’s device. To bolster its argument, Apple also pointed to another provision in CALEA, 47 U.S.C. § 1002(b)(1)(A), which says the statute does not authorize the government to require “any specific design of equipment, facilities, services, features, or system configurations” to be adopted by any provider of a wire or electronic communication service [or] any manufacturer of telecommunications equipment.” Apple argued that CALEA thus “prohibit[ed]” the government from requiring the company to design software to bypass the passcode-protection features on Farook’s device.

Apple also noted that under CALEA telecommunications carriers are not responsible for “decrypting, or ensuring the government’s ability to decrypt, any communication” unless the carrier already “possess[es]” a “decryption program.” If not even telecommunications carriers are required to assist law enforcement with decryption (subject to a narrow exception), Apple argued, then surely the government has no authority whatsoever to compel an entity exempt from CALEA’s requirements to decrypt.

Finally, Apple pointed out that Congress—at the FBI’s urging—had previously considered expanding CALEA to require entities beyond telecommunications carriers to retain the capability to provide law enforcement with access to their users’ communications but had declined, indicating that the FBI lacked the authority to compel other types of companies to facilitate the government’s decryption requests.

The government disputed Apple’s interpretation of CALEA. The government first argued that CALEA only addressed entities’ responsibilities with respect to “real-time interceptions” of communications, not access to “stored” data like Farook’s on-device iMessages. Therefore, CALEA was not directly on point, leaving the court free to exercise its residual authority under

---

113 Apple’s San Bernardino Reply Brief, supra note 107, at 7.
114 Id. at 9.
115 Id. at 8.
116 Id.
117 Id. at 9 n.8 (citing 47 U.S.C. § 1002(b)(3)).
118 Id. at 9-10.
119 See id. at 12; see also Charlie Savage, U.S. Tries to Make It Easier to Wiretap the Internet, N.Y. TIMES (Sept. 27, 2010), https://perma.cc/7Y6C-6V94.
120 Government’s San Bernardino Brief, supra note 78, at 22-23 (emphases added).
the All Writs Act.\textsuperscript{121} The government maintained that a statute must “specifically address[] the particular issue at hand” to deprive a court of its authority under the All Writs Act: “It is not enough for other laws to brush up against similar issues.”\textsuperscript{122} Congress’s inaction in response to the FBI’s lobbying for specific legislation expanding CALEA also could not be read as “persuasive” evidence that Congress disapproved of compelling Apple’s assistance in this case because “several other equally tenable inferences may be drawn from such inaction’ . . . including that Congress [was] satisfied with existing authorities.”\textsuperscript{123} More fundamentally, the government explained that CALEA was intended to “preserve the status quo” (i.e., to ensure that telecommunications carriers maintained the capability to intercept communications when ordered to), not to limit (nor expand) any of the government’s existing surveillance authorities.\textsuperscript{124}

EDNY Magistrate Judge Orenstein was persuaded by Apple’s arguments, finding that even if CALEA did not explicitly proscribe the government from requiring Apple to unlock Farook’s device, it likely was “part of a larger legislative scheme that is so comprehensive as to imply a prohibition” on such compelled assistance.\textsuperscript{125}

\textbf{iii. Outcome}

The FBI ended up withdrawing its requests in both the San Bernardino and EDNY cases after purchasing expensive third-party software capable of unlocking both suspects’ iPhones without Apple’s assistance.\textsuperscript{126} In light of the opposing magistrate orders, and because both cases were ultimately rendered moot and never subject to review by a district judge, let alone an appellate court, the scope of the government’s ability to leverage the All Writs Act to compel Apple’s technical assistance remains unsettled.

\begin{footnotesize}
\footnotesize
\begin{itemize}
\item \textsuperscript{121} Id. at 23.
\item \textsuperscript{124} See Government’s San Bernardino Reply Brief, \textit{supra} note 103, at 10 (quoting U.S. Telecom Ass’n v. F.C.C., 227 F.3d 450, 455 (D.C. Cir. 2000)).
\item \textsuperscript{125} EDNY Order II, \textit{supra} note 77, at 15-16.
\item \textsuperscript{126} Katie Benner & Eric Lichtblau, \textit{U.S. Says It Has Unlocked iPhone Without Apple}, \textit{N.Y. TIMES} (Mar. 28, 2016), https://perma.cc/M3TN-2C2M; Danny Yadron, ‘Worth it’: FBI admits it paid $1.3m to hack into San Bernardino iPhone, \textit{GUARDIAN} (Apr. 21, 2016, 4:33 PM EDT), https://perma.cc/CG8C-BG75.
\end{itemize}
\end{footnotesize}
Subsequent scholarship has generated additional arguments against Apple’s understanding of CALEA complimentary to those raised by the government in 2016. To begin, even if CALEA does extend to access to data at rest, the statute can be read as imposing additional obligations on telecommunications carriers without diminishing the existing legal obligations other kinds of communication service providers have under other statutes. That is, while CALEA does not require information service providers (as it does telecommunications carriers) to preemptively ensure their equipment, facilities, and systems enable law enforcement to access the contents of communications transmitted via their service, all communication service providers are still required to provide at least some degree of assistance to help the government access such communications. As the House Report on CALEA explained, “[i]nformation services can be wiretapped pursuant to court order, and their owners must cooperate when presented with a wiretap order, but these services and systems do not have to be designed so as to comply with the capability requirements.”

In addition, a closer look at the statutory language suggests CALEA’s reach may not be as broad as Apple contended. In its brief, Apple argued that CALEA “prohibit[ed]” and “forbade” the FBI from compelling the company to assist with gaining access to Farook’s on-device iMessages. However, the statute’s language (e.g., “this subchapter does not authorize” and “the requirements of subsection (a) do not apply to”) does not actually nullify other existing authorities. Rather, this language arguably fits with Congress’ stated purpose to neither diminish nor expand the government’s surveillance authorities, but merely preserve the status quo.

---

127 See, e.g., Steven R. Morrison, Breaking iPhones Under CALEA and the All Writs Act: Why the Government Was (Mostly) Right, 38 CARDOZO L. REV. 2039, 2065-68, 2071-72 (2017); Hurwitz, supra note 108, at 404 (arguing it is “unclear” whether CALEA’s exemptions are relevant to Apple v. FBI); Caren Morrison, Private Actors, Corporate Data and National Security: What Assistance Do Tech Companies Owe Law Enforcement?, 26 WM. & MARY BILL RTS. J. 407, 417 (2017) (“CALEA’s lessons on encryption are debatable at best.”).
128 See Caren Morrison, supra note 127, at 414-17.
129 CALEA HOUSE REPORT, supra note 108, at 18 (emphasis added).
130 Apple’s San Bernardino Reply Brief, supra note 107, at 8, 9.
131 47 U.S.C. § 1002(b)(1)(A) (clarifying that telecommunications carriers and other communication service providers are not required to design their equipment, facilities, services, features, or system in any specific way).
133 See CALEA HOUSE REPORT, supra note 108, at 22 (“The Committee intends the assistance requirements in section [1002] to be both a floor and a ceiling. The FBI Director testified that
Finally, with respect to the provision of CALEA that says that communication service providers are not required to adopt “any specific design,”134 the provision’s language seems to leave open the possibility that the government can require a company to expand an existing backdoor, so long as it does not mandate the creation of an entirely new backdoor.

C. Application to Communication Safety Scenario

The government could seek to leverage the All Writs Act to compel Apple to modify its Communication Safety feature to access the decrypted content of a suspect’s stored iMessages. The government’s ability to do so first turns on whether CALEA precludes a court from issuing an All Writs Act order in the first place, a still unsettled question of statutory interpretation. If CALEA controls, there is likely no way the government can compel Apple’s assistance.135 But as discussed, there are reasonable arguments that CALEA is not controlling.

If CALEA does not preclude the issuance of an All Writs Act order, the validity of such an order would turn on whether the three factors from New York Telephone Co. were satisfied. Benchmarked against the 2016 iPhone standoff, Apple’s introduction of Communication Safety bolsters the government’s case.

First, the requirement that the assistance be “essential to the fulfillment”136 of the government’s objectives would be easily satisfied. Law enforcement currently has no ability to access the decrypted content of a suspect’s messages unless the messages have been backed up to iCloud.137 Thus the only means of doing so would be to utilize a modified version of Apple’s Communication Safety tool.

Second, Apple would likely be sufficiently connected138 to the controversy that its assistance could be permissibly compelled. As the government argued in the San Bernardino iPhone case, the Supreme Court made clear in New York Telephone Co. that even “private citizens have a duty

---

135 See EDNY Order II, supra note 77, at 15-16.
137 Pfefferkorn, supra note 26 (citing a Jan. 7, 2021 FBI document).
138 See 434 U.S. at 174.
to provide assistance to law enforcement officials when it is required. . . .”

There would also be a clear nexus between Apple—the designer and licensor of the service (iMessage) used by the suspect in furtherance of criminal activity—and a government investigation that hinged in large part on successfully accessing the content of the suspect’s messages. In his order denying the FBI’s application in 2016, EDNY Magistrate Judge Orenstein claimed that nothing “even remotely suggests that the licensed [iOS] software played any meaningful role in [the suspect’s] [drug trafficking] crime comparable to the role the telephone company’s property played in the [gambling] crimes under investigation in N.Y. Tel. Co.” This would not necessarily be true, however, in the case of a criminal scheme that relied to a greater extent on communications among co-conspirators. Furthermore, the government could reasonably argue that iMessage and its encryption protocol play an integral role in a suspect’s criminal activity. While criminals are likely first drawn to iMessage due to the iPhone’s ubiquity, they may continue to use iMessage rather than shift to a different messaging service in part because of the known difficulty law enforcement encounters trying to access encrypted iMessages. Finally, the Court in New York Telephone Co. held that assistance could be required from “persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice . . . .” In the EDNY case, Magistrate Judge Orenstein determined that Apple had not “thwart[ed]” the government’s investigation by introducing passcode-protection features because it was the suspect himself who “engaged” the features. Yet unlike the iPhone’s passcode-protection features, a suspect does not “engage” iMessage’s encryption and has no means to disable it. Furthermore, the service’s encryption protocol solely and completely frustrates the court’s warrant and the government’s investigation. For these reasons, Apple would likely be sufficiently connected to the underlying controversy to satisfy the second All Writs Act requirement.

---

140 EDNY Order II, supra note 77, at 32.
141 434 U.S. at 174.
142 EDNY Order II, supra note 77, at 36.
143 Id. at 35.
The closest call is whether compelling Apple to modify its Communication Safety feature would impose an “unreasonable burden” on the company. In *New York Telephone Co.*, the Court determined that the requested assistance would not be unduly burdensome because it “required minimal effort on the part of the Company and no disruption to its operations.” With respect to the level of effort required from Apple, the inquiry would hinge on the technical specifics involved in expanding the Communication Safety feature. This issue would surely be fiercely litigated, but several experts have suggested that Apple could make similar modifications relatively easily. As the FBI also noted in the San Bernardino iPhone case, Apple routinely “writes software code as part of its regular business.”

Regarding the potential disruption to Apple’s services, the government would need to assure the court that the modified Communication Safety feature would only be pushed to the suspect’s device. A court would be unlikely to compel any modifications that would affect other iMessage users. Again, deciding this question would require a more comprehensive technical analysis, but it likely is not beyond Apple’s ability to push out a targeted, user-specific update.

A court could potentially compel Apple’s assistance even under a definition of burdensome that is relatively deferential to Apple. As litigation unfolded in the San Bernardino iPhone and EDNY cases, national security legal scholars Robert Chesney and Steve Vladeck argued that the burden factor should be read in such a way that compelling a company “to help the government utilize existing vulnerabilities in its software” is not considered unduly burdensome, but requiring it “to devote its resources to creating material new software vulnerabilities which can then be exploited by the

---

144 434 U.S. at 172.
145 434 U.S. at 175.
146 *See* [HAL ABELOE ET AL., BUGS IN OUR POCKETS: THE RISKS OF CLIENT-SIDE SCANNING 21 (2021),](https://perma.cc/NXY7-C7PV) (“[It] would be a minimal change to reconfigure the scanner on the device to report any targeted content . . . .”)); [Jonathan Mayer & Anunay Kulshrestha, We Built a System Like Apple’s to Flag Child Sexual Abuse Material — and Concluded the Tech Was Dangerous, WASH. POST](https://perma.cc/JDN5-G4F9) (“Our system could be easily repurposed for surveillance and censorship. The design wasn’t restricted to a specific category of content . . . .”).
148 *See* Nadim Kobeissi (@kaepora), [TWITTER](https://twitter.com/kaepora/status/1423387147172724741,https://perma.cc/9NDH-QKB6) (prominent cryptography expert and internet freedom advocate arguing, “Apple can trivially use different CSAM datasets for each user. For one user it could be child abuse, for another it could be a much broader category.’’).
government” is. While Apple would surely argue that modifying its Communication Safety feature would amount to the creation of new vulnerabilities, the government would have a reasonable argument that such assistance would make use of an existing loophole in iMessage’s encryption protocol.

In their 2016 standoff, Apple and the FBI disagreed as to whether the burden imposed on the company should be measured solely by “the direct costs of compliance” or also encompass more general consequences for Apple’s business. Apple argued that the hit it would endure to its reputation as a champion for user privacy and security if it were forced to assist the FBI qualified as a burden. While Magistrate Judge Orenstein was sympathetic to this view, indulging such a claim would create perverse incentives for companies to exaggerate their commitment to privacy as a cheap way to absolve themselves of responsibility to assist law enforcement. In addition, Apple would have a harder time claiming it safeguards users’ privacy at all costs after it has implemented a tool to scan child users’ iMessages for nudity.

In summary, benchmarked against the San Bernardino and EDNY cases, Apple’s introduction of Communication Safety weakens its argument that a court lacks the authority to compel its assistance under the All Writs Act. Most importantly, it undercuts Apple’s claim that searching the unencrypted contents of a suspect’s iMessages would be unduly burdensome, as the Communication Safety feature provides the preliminary architecture to do so and could conceivably be expanded with reasonable efforts.

Lastly, in the San Bernardino iPhone case, Apple also asserted a fallback First Amendment claim, arguing that the government’s attempt to compel

---

150 Government’s San Bernardino Brief, supra note 78, at 16.
151 See Apple’s San Bernardino Brief, supra note 75, at 23 (“Apple has a strong interest in safeguarding its data protection systems that ensure the security of hundreds of millions of customers who depend on and store their most confidential data on their iPhones. An order compelling Apple to create software that defeats those safeguards undeniably threatens those systems and adversely affects Apple’s interests and those of iPhone users around the globe.”).
152 EDNY Order II, supra note 77, at 43-44.
153 See David S. Kris, Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond, 8 J. Nat’l Sec. & Pol’y 377, 408 (2016) (“Taken to its logical conclusion, this might mean that a provider could create its own undue burden by strongly and publicly opposing assistance with governmental surveillance.”).
Apple to write code was tantamount to unconstitutional compelled speech.\(^{154}\) Apple could similarly try to argue that compelled technical adaptations to its Communication Safety feature amount to compelled speech. A full analysis of the merits of this claim is beyond the scope of this Note. However, courts would probably be reluctant to sustain such a claim, as doing so might call into question the constitutionality of other statutes that mandate technical assistance, including CALEA and the Wiretap Act.

IV. REAL-TIME INTERCEPTION OF iMESSAGES PURSUANT TO A WIRETAP ACT OR FISA ORDER

In a slight variation to the scenario explored in Part III, the government could also seek to surveil a suspect’s iMessages in real time. Real-time interception of iMessages is wholly impeded by the service’s encryption protocol,\(^{155}\) but this may have changed with Apple’s introduction of Communication Safety. While the government must meet a high bar to obtain authorization for real-time interception of communications,\(^{156}\) there are reasons the government may prefer this approach. For one, repurposing Apple’s Communication Safety feature for real-time surveillance might require fewer technical modifications than altering the system to scan stored iMessages, as the system is already designed to scan child users’ iMessages for nudity in real time. In addition, suspects often routinely delete messages upon delivery or receipt, making real-time interception more imperative.

Real-time surveillance of communications is governed by different statutory authorities—the Wiretap Act and the Foreign Intelligence Surveillance Act (FISA)—than those covering access to data at rest discussed in Part III. As a preliminary matter, because there are statutes that specifically address real-time surveillance, the government would not be able to leverage

---

\(^{154}\) Apple’s San Bernardino Brief, supra note 75, at 32-33 (citing Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 662 (1994); Universal City Studios, Inc. v. Corley, 273 F.3d 429, 449 (2d Cir. 2001)).

\(^{155}\) See Pfefferkorn, supra note 26 (citing FBI document); McCullagh & Van Grove, supra note 26 (citing DEA document).

\(^{156}\) Among other requirements, to obtain a Wiretap Act order, the government must demonstrate that “normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.” 18 U.S.C. § 2518(3)(c). For this reason, Wiretap Act orders are sometimes referred to as “super warrants.” See, e.g., Jennifer S. Granick et al., Mission Creep and Wiretap Act ‘Super Warrants’: A Cautionary Tale, 52 LOY. L.A. L. REV. 431 (2019).
a court’s residual authority under the All Writs Act.157 Instead, the Wiretap Act and FISA each contain provisions that enable the government, upon obtaining a court order, to compel service providers to assist with the interception of a suspect’s communications. Under the Wiretap Act, the government may “direct that a provider of wire or electronic communication service . . . shall furnish . . . all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the service.”158 Under FISA Title I, which regulates electronic surveillance of persons located within the United States who are believed to be agents of a foreign power, a communication provider must “furnish the [government] forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference.”159 The compelled assistance provisions of the Wiretap Act and FISA Title I are each subject to a modest limitation: the information, facilities, or technical assistance requested from the provider must not result in more than a “minimum of interference” with the provider’s service.

The publicly available case law adjudicating the scope of the Wiretap Act and FISA’s compelled assistance provisions is relatively scarce and limited to cases involving the Wiretap Act and Pen Register and Trap and Trace Act (which contains analogous compelled assistance provisions).160 No FISA order concerning compelled assistance has been declassified and published, if one exists.161 Nevertheless, the following review of the available case law indicates that the government might be able to successfully leverage the Wiretap Act or FISA to compel Apple to repurpose its Communication Safety feature to surveil a suspect’s iMessages.

---

157 Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985) (“The All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute. Where a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling.”).
160 See Kris, supra note 153, at 407.
161 At least one commentator has inferred from privacy-conscious legislators’ actions that the government has utilized or plans to utilize FISA’s compelled assistance provision extensively. See Marcy Wheeler, Ron Wyden Is Worried the Government Will Use FISA Process to Force Companies to Make Technical Changes, EMPTYWHEEL (Oct. 24, 2017), https://perma.cc/CMN9-2LJ2.
A. Car Eavesdropping Case: Minimum of Interference Limitation

In 2003, the Ninth Circuit sustained a challenge to a series of district court orders directing a car manufacturer, under the compelled assistance provision of the Wiretap Act,\(^\text{162}\) to assist the FBI with eavesdropping on a suspect’s conversations by repurposing the theft recovery feature embedded in the suspect’s vehicle.\(^\text{163}\) The vehicle was equipped with a service that, when turned on (normally after the owner reported the vehicle stolen), enabled the manufacturer to establish an audio feed to the vehicle.\(^\text{164}\) The FBI obtained a warrant to monitor the suspect’s communications in the suspect’s vehicle and then sought to compel the vehicle manufacturer to turn on the remote audio feed feature to accomplish the surveillance.\(^\text{165}\) The Ninth Circuit considered whether the surveillance could be achieved with a “minimum of interference” with the service.\(^\text{166}\) The Court ultimately held that it could not.\(^\text{167}\) While declining to define the precise scope of “minimum of interference,” the Court explained, “A ‘minimum of interference’ at least precludes total incapacitation of a service while interception is in progress.”\(^\text{168}\)

The Court determined that complying with the FBI’s request to repurpose the vehicle’s audio feed would result in a “complete disruption” to the manufacturer’s service.\(^\text{169}\) First, while the remote audio feature was engaged, the vehicle’s non-emergency services could not be used at all.\(^\text{170}\) Second, the vehicle’s emergency button would be effectively disabled as well.\(^\text{171}\) Normally, pressing the emergency button would connect the vehicle occupant to an operator that could alert the police or medical personnel of an emergency, but with the audio connection already established and the feed being only intermittently monitored by the FBI instead of a trained operator, the emergency assistance function would be worthless.\(^\text{172}\) The Court determined that this disruption to the service constituted more than a “minimum of interference,” and therefore held that the manufacturer was not


\(^{163}\) The Company v. United States, 349 F.3d 1132, 1146 (9th Cir. 2003).

\(^{164}\) Id. at 1134.

\(^{165}\) Id.

\(^{166}\) Id. at 1137-46.

\(^{167}\) Id. at 1146.

\(^{168}\) Id. at 1145 (emphasis added).

\(^{169}\) Id.

\(^{170}\) Id. at 1135, 1146.

\(^{171}\) Id. at 1146.

\(^{172}\) Id.
required to render the assistance requested by the FBI.\textsuperscript{173} The Court also noted that the manufacturer, as a non-telecommunications carrier, was not required by CALEA to redesign its system to facilitate the surveillance in a manner that would result in less interference.\textsuperscript{174}

In dissent, Judge Richard C. Tallman disagreed with the majority’s interpretation of the “minimum of interference” limitation.\textsuperscript{175} Rather than requiring that the surveillance not result in any significant disruption to a communication service, he argued that the standard merely required that the surveillance be executed in a manner that “causes the least amount of disruption necessary to intercept the targeted communication.”\textsuperscript{176} “Minimum of interference,” is a “relative standard,” not an “absolute threshold,” he concluded.\textsuperscript{177} As such, the vehicle manufacturer could be compelled to turn on the remote audio feed so long as there was no less disruptive means of carrying out the surveillance.\textsuperscript{178}

\begin{enumerate}
\item \textbf{B. United States v. Lavabit: Furnishment of Information and Assistance}
\end{enumerate}

In 2014, the Fourth Circuit upheld on procedural grounds a contempt order against the encrypted email service Lavabit stemming from the company’s repeated refusal to comply with a duly issued order under the Pen Register and Trap and Trace Act.\textsuperscript{179} The government had obtained an order under the statute to capture real-time metadata associated with a Lavabit account later confirmed\textsuperscript{180} to belong to National Security Agency (NSA) whistleblower Edward Snowden.\textsuperscript{181} Like the Wiretap Act and FISA Title I, the Pen Register and Trap and Trace Act also contains provisions requiring a provider of an electronic communication service to, in the case of a pen register,\textsuperscript{182} furnish the government with “all information, facilities, and

\begin{footnotes}
\item Id.
\item Id. at 1146 n.27.
\item 349 F.3d at 1147.
\item Id.
\item Id. at 1148.
\item Kim Zetter, \textit{A Government Error Just Revealed Snowden Was the Target in the Lavabit Case}, \textit{WIRED} (Mar. 17, 2016, 5:30 PM), https://perma.cc/6RVA-QJ3K.
\item 749 F.3d at 280-81.
\item A pen register captures metadata of outgoing calls/messages.
\end{footnotes}
technical assistance necessary to accomplish the installation of the pen register” and, in the case of a trap-and-trace device, furnishes “all additional information, facilities and technical assistance including installation and operation of the device.” The Act contains the same limitation as in the Wiretap Act and FISA that the provider’s assistance is only required if it can be accomplished with a “minimum of interference” with the service.

Lavabit’s email service encrypted users’ data both in storage on Lavabit’s servers and while in transit (“transport encryption”). Lavabit’s transport encryption utilized an industry-standard protocol called SSL (Secure Sockets Layer). This encryption obstructed the government’s ability to acquire the metadata it ordinarily obtains from a pen register or trap-and-trace device. Importantly, however, Lavabit retained the private keys necessary to decrypt its users’ data. The FBI—citing the compelled assistance provisions of the Pen Register and Trap and Trace Act and the required disclosure provision of the Stored Communications Act (SCA)—therefore sought to compel Lavabit to hand over its private keys so that investigators could successfully install the court-authorized pen register and trap-and-trace device on Snowden’s account and decrypt the account’s metadata. The district court issued a Pen/Trap Order and later a seizure warrant for the decryption keys under the SCA. When Lavabit refused to comply, the district court held Lavabit and its owner in civil contempt and imposed monetary sanctions.

Lavabit challenged the district court’s contempt order. On appeal, it argued that the compelled assistance provisions of the Pen Register and Trap

---

183 A trap-and-trace device captures metadata of incoming calls/messages.
184 18 U.S.C. § 3124(a), (b).
185 Id.
186 749 F.3d at 279.
187 Id. at 280.
189 749 F.3d at 280.
190 Id. at 280-83.
191 Id. at 280-82.
192 At one point, Lavabit provided the FBI with an 11-page printout in 4-point font, which it claimed contained the requested encryption keys. The government subsequently requested that Lavabit provide the keys in industry-standard electronic format. Id. at 284.
193 Id. at 280.
and Trace Act and the required disclosure provision of the SCA did not obligate Lavabit to turn over its decryption keys. Lavabit argued that the statute merely required the company to install the authorized pen register and trap-and-trace device, but not to provide information or technical assistance to make the devices effective. “Encryption keys are not necessary to install the device,” Lavabit argued, and Congress never intended to compel such assistance. Lavabit also argued that turning over its decryption keys would compromise the communications of all its users, not just the target account, in violation of the Fourth Amendment’s particularity requirement.

The government countered by arguing that the statutory language of the compelled assistance provisions in the Pen Register and Trap and Trace Act plainly obligated Lavabit to turn over its decryption keys. The text of the trap-and-trace provision, the government explained, requires a provider to furnish “all additional information” necessary for the “installation and operation” of the device. The government argued that “information” clearly included the decryption keys in Lavabit’s possession, which were essential to the device’s operation. With respect to the pen register, the government also pointed to the text of its governing provision, which requires a provider to furnish “all information, facilities, and technical assistance necessary to accomplish the installation of the pen register.” Note that whereas the trap-and-trace provision mentions installation and operation, the pen register provision only mentions installation. Nonetheless, the government argued that the decryption keys were also critical “information” to the pen register’s installation, because “[a] device that cannot decode dialing, routing, addressing, or signaling information is simply not a pen register; thus, without

194 Brief of Appellant at 14-21, United States v. Lavabit, LLC 749 F.3d 276 (4th Cir. 2014) (Nos. 13-4625(L), 13-4626).
195 Id. at 14-15.
196 Id. at 15.
197 Id. at 26 (“Just as the government cannot demand the master key to every room in a hotel based on probable cause to search for evidence of a particular guest’s crime . . . the government cannot seize Lavabit’s private keys to expose and search through the content and non-content data of all its users.”).
199 Id. at 23-24 (citing 18 U.S.C. § 3124(b) (emphasis added)).
200 Id. at 24.
201 Id. at 25-26 (citing 18 U.S.C. § 3124(a)).
Lavabit’s encryption keys, no pen register could be installed on the targeted account at all.” In other words, without the means to decrypt the target account’s metadata, the government would be installing a useless device, not a pen register, so the text of the provision compelling a provider to assist with a pen register’s installation extended to Lavabit turning over its decryption keys.

The Fourth Circuit ultimately punted on the dispute. Because Lavabit failed to challenge the Pen/Trap Order at the trial court level (limiting the appellate court’s review to plain error) and then did not allege anywhere in its appellate briefs or at oral argument that the district court’s interpretation of the compelled assistance provisions constituted plain error, the Fourth Circuit determined that it was precluded from ruling on the scope of the provisions, as Lavabit “[fail[ed]] to identify any potential ‘denial of fundamental justice’ that would justify further review.” Thus the question of whether, and in what circumstances, the government can compel a provider’s assistance with decryption was left for another day.

C. Facebook Messenger Case: A Broader View of “Minimum of Interference”?

In August 2018, Reuters reported that in a sealed proceeding in the Eastern District of California, the government had sought a court order under the Wiretap Act to compel Facebook to assist with decrypting suspects’ voice communications via Facebook Messenger. The case arose from an investigation into suspected members of the MS-13 gang. The FBI sought to listen in on the suspects’ voice conversations using Messenger, but was stymied by Messenger’s encryption protocol for voice calls. The judge ultimately

---

204 United States v. Lavabit, LLC 749 F.3d 276, at 292-93 (“[O]ur review is circumscribed by the arguments that Lavabit raised below and in this Court.”).
207 Id.
208 Id. Facebook does not employ end-to-end encryption by default for plain text messages and reportedly has delayed plans to do so at the request of the U.S., U.K., and Australian governments. See Dan Milmo, Meta Delays Encrypted Messages on Facebook and Instagram to 2023, THE GUARDIAN (Nov. 21, 2021, 7:12 EST), https://perma.cc/AV2X-32XU; William P. Barr et al., Open Letter to Facebook (Oct. 4, 2019), https://perma.cc/SUSK-QKKC.
ruled against the government, declining to compel Facebook to “break” its service’s encryption.209 Because the case remains sealed,210 we are left to speculate as to the considerations the court weighed in reaching its decision. However, leaked details from the proceedings and expert commentary helps shed light on some of the factors likely at play.

Facebook reportedly argued that it had no readily available means to decrypt the suspects’ voice communications, so complying with the government’s request would require the company to rewrite its code—an action that exceeded the scope of its obligations under the compelled assistance provision of the Wiretap Act.211 As previously discussed, the provision’s only real limitation is that the assistance, if it is to be compelled, must be achievable with a “minimum of interference” with the service.212 In the Ninth Circuit car eavesdropping case, the court assessed the limitation in the narrow context of whether the service itself would be disrupted.213 However, some experts have suggested “minimum of interference” could potentially be interpreted more broadly to include whether complying with the government’s request would disrupt other users’ experience, saddle the provider with excessive expenses, or weaken the security of the service generally.214

Research by experts found that at the time of the case215 Facebook Messenger’s voice and video calling services utilized an encryption protocol called S-DES (Simplified Data Encryption Standard).216 Accordingly, when a Messenger user made a voice call to another, the data was encrypted in transit

209 Ellen Nakashima, Facebook Wins Court Battle over Law Enforcement Access to Encrypted Phone Calls, Wash. Post (Sept. 28, 2018), https://perma.cc/75RY-LTZK.
210 United States DOJ v. ACLU Found., 812 F. App’x 722, 724 (9th Cir. 2020) (declining to unseal records from the proceedings).
211 Nakashima, supra note 209.
213 The Company v. United States, 349 F.3d at 1145 (9th Cir. 2003).
214 See Jennifer Granick (@granick), Twitter (Aug. 17, 2018, 8:01 PM), https://twitter.com/granick/status/1030605565154619393, https://perma.cc/L9VN-HWZ6; cf. Kris, supra note 153, at 407 (“In general, the ‘technical assistance’ requirement admits of a balancing of the provider’s costs and burdens on the one hand against governmental need and alternatives on the other.”).
using a session key.\textsuperscript{217} Most of the call data was not routed through Facebook’s central servers, except for a limited amount when the call was first initiated, including—critically—the call’s session key.\textsuperscript{218} This meant that Facebook potentially had the ability to capture a call’s session key, enabling it to decrypt a user’s voice communications.\textsuperscript{219} However, doing so would certainly have required some technical maneuvers. It is possible the court determined that such technical modifications would amount to more than a “minimum of interference” with the service, perhaps because they would require excessive resources from Facebook or could only be achieved by compromising the security of other users’ calls. A broader interpretation of “minimum of interference” might explain the court’s ruling against the government.

Another issue speculated to have come up during the proceedings was whether Facebook Messenger was covered by CALEA’s assistance capability provision\textsuperscript{220} and thereby required to proactively design its service in a way that enabled the interception of communications.\textsuperscript{221} In 2005, the Federal Communications Commission (FCC) extended CALEA’s requirements to certain Voice over Internet Protocol (VoIP) services.\textsuperscript{222} The D.C. Circuit subsequently affirmed the FCC’s decision.\textsuperscript{223} However, the FCC excluded from its rule purely internet-based services.\textsuperscript{224} This was likely because Congress specifically exempted “information services” from CALEA.\textsuperscript{225} As such, Facebook Messenger is almost certainly exempt from CALEA’s requirements.

\textbf{D. Application to Communication Safety Scenario}

To contest an order under the Wiretap Act or FISA compelling the company to repurpose its Communication Safety feature to surveil a suspect’s

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{217} Brandom, supra note 216.
\item \textsuperscript{218} Id.
\item \textsuperscript{219} Id.
\item \textsuperscript{220} 47 U.S.C. § 1002.
\item \textsuperscript{221} See Levine & Menn, supra note 206; Tim Cushing, DOJ Asking Court To Force Facebook To Break Encryption On Messenger Voice Calls, TECHDIRT (Aug. 20, 2018), https://perma.cc/72LR-JQRF.
\item \textsuperscript{222} Communication Assistance for Law Enforcement Act and Broadband Access and Services, 70 Fed. Reg. 59664 (Oct. 13, 2005) (to be codified at 47 C.F.R. § 64.2102) [hereinafter FCC CALEY Rule].
\item \textsuperscript{223} Am. Council on Educ. v. F.C.C., 451 F.3d 226, 236 (D.C. Cir. 2006).
\item \textsuperscript{224} FCC CALEY Rule, supra note 222, ¶ 75 (“[C]ertain VoIP service providers are not subject to CALEY obligations imposed in today’s 1st R&O. Specifically, the 1st R&O does not apply to those entities not fully interconnected with the [public switched telephone network].”).
\item \textsuperscript{225} See 47 U.S.C. § 1002(b)(2).
\end{itemize}
\end{footnotesize}
iMessages in real time, Apple would likely first raise many of the same CALEA-related arguments as it did in the San Bernardino iPhone case. As discussed, however, it is not certain these arguments would succeed. Assuming they would not, the validity of such a Wiretap Act or FISA order would turn on whether the requested assistance would exceed the limitations on the government’s authority as specified in both statutes.

First, repurposing the Communication Safety feature would not result in a “complete disruption” to iMessage, unlike the assistance sought in the Ninth Circuit car eavesdropping case. Especially if a court adopted Judge Tallman’s less stringent interpretation of “minimum of interference,” the government would likely have little difficulty convincing a court that an order compelling Apple to use the feature to intercept a suspect’s iMessages would not violate this particular constraint imposed by Congress.

Second, the district court’s contempt order in Lavabit and the Fourth Circuit’s upholding of the order (albeit on procedural grounds) lends modest support to the proposition that a provider, if it possesses a means of decrypting a user’s communications, could be compelled under the Wiretap Act or FISA to employ such means at the government’s behest. Apple’s Communication Safety feature arguably gives it such means. Even privacy advocates have acknowledged that if a company builds a backdoor to its service’s encryption, it can likely be compelled by the government to utilize it. Furthermore, unlike in Lavabit, the requested decryption could probably be confined to only the suspect’s account, leaving other iMessage users unaffected, as discussed in Part III.C.

One hurdle the government might need to overcome is that, whereas in Lavabit the government requested that the provider furnish information (decryption keys), Apple would be asked to furnish technical assistance (modified software) in this scenario. The language of the Wiretap Act and FISA does not place greater limits on the furnishment of technical assistance than

---

226 See *supra* text accompanying notes 127-134 (discussing arguments against Apple’s interpretation of CALEA).
229 See *supra* text following note 147.
information. However, in *New York Telephone Co.*, the Supreme Court held that “unreasonable burdens may not be imposed” on third parties, whether under the All Writs Act or another statute.\textsuperscript{230} Thus, Apple could try to argue that furnishing technical assistance is inherently more burdensome than furnishing information and therefore the government is more constrained in its ability to compel such assistance. This would be in line with the broader view of “minimum of interference” suspected to have been adopted by the court in the Facebook Messenger case.

The Facebook Messenger case is a strong data point in Apple’s favor. However, there are ways to possibly distinguish the assistance sought in that case from an order compelling Apple to modify its Communication Safety feature. On the spectrum of difficulty, Apple modifying the feature would certainly be more burdensome than Lavabit simply handing over decryption keys in its possession, but perhaps less technically onerous than Facebook capturing a Messenger call’s session key. It is not Facebook’s practice to decrypt its users’ voice calls, whereas it is now Apple’s practice—if the Communication Safety feature is engaged—to monitors some of its users’ iMessages for a specific type of content.

With little publicly available case law to go off and reasonable arguments on both sides, it is difficult to predict with any certainty how the government would ultimately fare if it attempted to leverage a Wiretap Act or FISA order to compel Apple to modify its Communication Safety feature to surveil a suspect’s iMessages in real time. But Apple’s introduction of the feature surely makes it a closer question than if the company had not deployed the feature.

V. CONCLUSION

This Note explored whether the U.S. government could compel Apple under existing legal authorities to repurpose its recently introduced Communication Safety feature to access the decrypted content of a suspect’s iMessages. It remains uncertain how a court would ultimately rule in such a scenario, but Apple’s deployment of the feature makes it more likely that the government would prevail.

Legislation proposed in Congress would either greatly disincentivize end-to-end encryption or definitively provide the government with the

\textsuperscript{230} See 434 U.S. at 172.
authority to order decryption. The EARN IT Act, reintroduced by Republican Senator Lindsey Graham and Democratic Senator Richard Blumenthal in late January 2022, would indirectly discourage companies from deploying end-to-end encryption by amending Section 230 of the Communications Decency Act to permit civil claims and state criminal charges against communication service providers that fail to take adequate steps to prevent CSAM.\textsuperscript{231} More directly, the Lawful Access to Encrypted Data Act, introduced by three Republican senators in June 2020, would “require device manufacturers and service providers to assist law enforcement with accessing encrypted data if assistance would aid in the execution of [a] warrant.”\textsuperscript{232}

U.S. allies have already passed similar legislation. In 2016, the U.K. enacted the Investigatory Powers Act, which included a provision authorizing the government to compel communication service providers to remove “electronic protection applied . . . to any communications or data.”\textsuperscript{233} The U.K. government has thus far refrained from utilizing such authority, however.\textsuperscript{234} The Australian government was given expansive authority to compel decryption in the 2018 Telecommunications and Other Legislation Amendment (Assistance and Access) Act.\textsuperscript{235} As of August 2020, Australian authorities had not yet used either of the compulsory mechanisms at their disposal to compel companies to utilize existing technological capabilities or build new ones to decrypt a suspect’s communications.\textsuperscript{236} However, as of November 2019, Australian authorities had issued at least twenty-five “voluntary” notices.\textsuperscript{237} The European Commission also recently published a draft regulation that would require communication service providers to comply with court orders, issued at the


request of national governments, directing them to scan users’ messages for CSAM.\textsuperscript{238}

The most serious threat to encryption is posed by authoritarian governments that are not constrained by any constitutional or statutory limitations. It is one thing for a U.S. law enforcement agency to obtain a court order compelling a company to assist with decryption after showing probable cause that a suspect is using the company’s service to engage in criminal activity, and entirely another for such an order to be issued with no independent judicial oversight. Given the unchecked power authoritarian regimes wield and their strong incentive to engage in censorship and discriminatory surveillance, companies must think hard before building anything that remotely resembles a backdoor into their encrypted communication services, even for noble purposes. Should they do so, it will not be long before governments seek to use it.\textsuperscript{239} Companies seeking to preserve the privacy and security benefits of encryption while still addressing the harms perpetrated using their services may find such a middle ground elusive.


\textsuperscript{239} See Green & Stamos, supra note 8 (“While Apple is introducing the child sexual abuse detection feature only in the United States for now, it is not hard to imagine that foreign governments will be eager to use this sort of tool to monitor other aspects of their citizens’ lives—and might pressure Apple to comply. Apple does not have a good record of resisting such pressure in China, for example, having moved Chinese citizens’ data to Chinese government servers. Even some democracies criminalize broad categories of hate speech and blasphemy. Would Apple be able to resist the demands of legitimately elected governments to use this technology to help enforce those laws?”).