VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SPRING 2019 UNIVERSITY OF VIRGINIA VOL. 22, NO. 04

The International Front of the Going Dark Debate

ERIC MANPEARL[1]

[1] Law Clerk to The Honorable Royce C. Lamberth of the United States District Court for the District of Columbia. J.D. 2018, The University of Texas School of Law; Master of Public Affairs 2018, Lyndon B. Johnson School of Public Affairs; B.A. 2013, Rice University. Eric Manpearl was previously the Brumley Next Generation Senior Graduate Fellow in the Intelligence Studies Project at the Robert S. Strauss Center for International Security and Law. Eric Manpearl also previously served as a Summer Law Clerk with the Office of the General Counsel at the Defense Intelligence Agency, Legal Counsel Division of the Office of the General Counsel at the Department of Homeland Security, and Office of Legal Policy at the Department of Justice. Special thanks to Professors Robert Chesney and Matt Tait for their thoughtful and invaluable suggestions, guidance, and advice. The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

TABLE OF CONTENTS

I. INTRODUCTION

The encryption debate has re-emerged in recent years with major security implications. This debate has become part of the larger discussion about balancing changing technological capabilities, security threats, and the evolution of society's sense of privacy. The types of encryption at the heart of this debate are end-to-end encryption and endpoint encryption—also called device encryption. End-to-end encryption is the encryption of messages in transit such that only the original sender and intended recipient hold the keys to decrypt the communication.[2] The message in transit can therefore only be read by the original sender and intended recipient. This type of encryption is important for protecting data in motion. Device encryption is when the keys only exist on locked devices, which prevents the contents of the device from being read by anyone who does not possess the keys.[3] This type of encryption is important for protecting stored information—data at rest.

The private sector and security officials have expressed numerous reasons why they oppose a lawful access requirement for either device encryption or encryption of messages in transit. The most prominent among these arguments is the fear that the technological architecture that would guarantee law enforcement and intelligence agencies access would compromise user security and privacy. The greatest potential harm from requiring lawful access for either device encryption or encryption of messages in transit may be the possible decrease in the market share and economic viability of U.S. companies. U.S. technology companies are an extremely important part of the U.S. economy and economic strength is an important aspect of national security as it enables countries to have geopolitical influence. Therefore, it is important to consider the economic interests of U.S. businesses when considering whether a lawful access requirement for either device encryption or encryption of messages in transit is appropriate. This aspect of the debate has not been analyzed enough, and this Article examines the encryption debates in France, Germany, the United Kingdom,

[2] MATTHEW G. OLSEN ET AL., DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE 4 (2016).
[3] *Id.*

China, and Russia to shed light on whether there are actually viable companies and markets outside the U.S. that could threaten U.S. companies if the United States imposed a lawful access requirement for either device encryption or encryption of messages in transit.

Part I discusses the current encryption debate in the United States. This part briefly examines the arguments on both sides of the "going dark" debate. Part II analyzes the encryption debates in France, Germany, the United Kingdom, China, and Russia. Finally, Part III considers the implications of these overseas encryption debates on the debate here in the United States. Ultimately, this Article concludes that U.S. technology companies appear unlikely to lose market share or economic viability as a result of a lawful access requirement for device encryption, but U.S.-based encrypted communications applications could suffer a great deal or decide to relocate to another country, such as Germany, as a result of a lawful access requirement for encryption of messages in transit.

II. THE ENCRYPTION DEBATE IN THE UNITED STATES

There is currently a very robust debate over whether there should be a lawful access requirement for either device encryption or encryption of messages in transit to mandate that companies maintain access to users' communications and data, and provide law enforcement or intelligence agencies with access upon receipt of a lawful order. Two recent developments have spurred the re-emergence of the encryption debate, which first came to a head with the "Crypto Wars" in the 1990s.[4] First, encryption is increasingly becoming the default setting on devices.[5] Data was formerly stored on devices in an unencrypted form unless the user took affirmative action to use encryption.[6] Now, however, more devices will encrypt

[4] *See, e.g.*, DANIELLE KEHL, ANDI WILSON & KEVIN BANKSTON, DOOMED TO REPEAT HISTORY? LESSONS FROM THE CRYPTO WARS OF THE 1990S 2–5 (2015) (recounting the history of the encryption debate).
[5] THE CHERTOFF GROUP, THE GROUND TRUTH ABOUT ENCRYPTION 1 (2016).
[6] *Id.*

data by default unless the user takes affirmative action to turn this function off and store data in an unencrypted form.[7] Thus, the burden of action formerly favored not using encryption, whereas now the burden of action will favor using encryption. This will greatly increase the prevalence of device encryption. Apple has been a leader in promoting default device encryption. In 2014, Apple announced it would include default encryption of its devices that use the iOS 8 mobile operating system.[8] Google followed suit by making encryption the default on its Android operating system.[9]

Second, service providers are offering end-to-end encryption on products and encrypting data that is stored in cloud storage systems.[10] These products encrypt data, information, and communications in such a way that the service provider does not have the technical capability to decrypt the information.[11] Therefore, these providers cannot respond to lawful process because they do not possess the information that the government is requesting.[12] In 2016, WhatsApp, an online messaging service on smartphones that is now owned by Facebook, implemented end-to-end encryption to its service, which is used by over 1 billion people.[13] Other applications that have also implemented end-to-end encryption have become popular recently, too.

A. LAW ENFORCEMENT AND INTELLIGENCE CONCERNS

[7] *Id.*
[8] *See* David E. Sanger & Brian X. Chen, *Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.*, N.Y. TIMES (Sept. 26, 2014), http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html (detailing Apple's new use of default encryption).
[9] *See id.* (noting Google's switch to default encryption).
[10] THE CHERTOFF GROUP, *supra* note 5, at 1.
[11] *Id.*
[12] *Id.*
[13] Andy Greenberg, *WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users*, WIRED (Nov. 18, 2014), https://www.wired.com/2014/11/whatsapp-encrypted-messaging/; Cade Metz, *Forget Apple vs. The FBI: WhatsApp Just Switched on Encryption for a Billion People*, WIRED (Apr. 5, 2016), https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/.

The Federal Bureau of Investigation (FBI) has led the government's involvement in the current debate since 2010.[14] The FBI is concerned that it is "going dark" because there is an increasing number of electronic communications that the FBI has the legal authority to intercept or obtain, but cannot feasibly do so.[15] Reports have indicated that encryption and other technological means, like proxy servers, can conceal information from lawful electronic surveillance.[16] Intelligence agencies, especially the National Security Agency (NSA) and Central Intelligence Agency (CIA), also face difficulties in fulfilling their missions of gathering intelligence because of encryption.[17] The NSA and CIA have greater resources to combat this problem than the FBI, though. Further, the "going dark" problem is most acute for state and local law enforcement agencies that have fewer resources than federal law

[14] *See* Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES (Sept. 27, 2010) http://www.nytimes.com/2010/09/27/us/27wiretap.html (discussing the FBI's initial efforts to address the growing concerns that investigators will lose the ability to intercept communications they are lawfully authorized to intercept).

[15] *See generally Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. (2011) (examining the "growing gap between the legal authority and the technical capability to intercept electronic communications").

[16] *See generally* FEDERAL BUREAU OF INVESTIGATION SITUATIONAL INFORMATION REPORT, GOING DARK: LAW ENFORCEMENT PROBLEMS IN LAWFUL SURVEILLANCE (2011) (explaining the problems that new technologies are posing for lawfully-authorized electronic surveillance).

[17] *See* Anna Mulrine, *New encryption technology is aiding terrorists, intelligence director says*, CHRISTIAN SCI. MONITOR (Apr. 25, 2016), http://www.csmonitor.com/USA/Politics/monitor_breakfast/2016/0425/New-encryption-technology-is-aiding-terrorists-intelligence-director-says (reporting on James Clapper's, the Director of National Intelligence, comments regarding encryption inhibiting the intelligence community's ability to collect intelligence, especially against terrorists); *CIA Director John Brennan on 60 Minutes*, CBS NEWS (Feb. 14, 2016), http://www.cbsnews.com/news/cia-director-john-brennan-60-minutes-scott-pelley/ (stating that encryption has hampered the CIA's ability to collect intelligence on ISIS); Michael Isikoff, *NSA chief: 'Paris would not have happened' without encrypted apps*, YAHOO (Feb. 17, 2016), https://www.yahoo.com/news/nsa-chief-paris-would-not-have-happened-without-184040933.html (Admiral Michael Rogers, Commander of U.S. Cyber Command and Director of NSA, warned encryption is making it more difficult for the NSA to intercept communications and fulfill its mission).

enforcement.[18] Nonetheless, there is concern across law enforcement and intelligence agencies about "going dark," and these agencies at all levels of government "would benefit if technological architectures did not present a barrier to investigations."[19]

Ultimately, law enforcement and intelligence agencies fear that they will not be able to prevent terrorist attacks, investigate crimes, and prosecute criminal activity without access to communications. Former FBI Director James Comey, who was very vocal in describing the "going dark" problem during his tenure as FBI Director, stated,

> [u]nfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem . . . 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. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.[20]

Without a lawful access requirement, there will be crimes that go unsolved that otherwise may have been solvable, and criminals will not be brought to justice.

Cyrus Vance, Jr., the Manhattan District Attorney, has testified that seventy-four cases in Manhattan from October 2014 to

---

[18] Adam Segal & Alex Grigsby, *How to break the deadlock over data encryption*, WASH. POST (Mar. 13, 2016), https://www.washingtonpost.com/opinions/how-to-break-the-deadlock-over-data-encryption/2016/03/13/e677fb78-d110-11e5-88cd-753e80cd29ad_story.html?utm_term=.0a2efccf86e8 ("The challenge of 'going dark' affects state and local law enforcement the most: They are the least likely to have the resources and technical capabilities to decrypt data relevant to an investigation.").

[19] OLSEN, *supra* note 2, at 6.

[20] James B. Comey, Dir., Fed. Bureau of Investigation, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, (Oct. 16, 2014), *available at* http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

June 2015 were hindered because law enforcement was unable to access information on a device because of device encryption.[21] Vance's office later updated this number to 423 devices lawfully seized from October 2014 to October 2016 in which law enforcement's investigation was hampered by device encryption.[22] These data are just from one district in a single state. The Harris County District Attorney's Office, in which Houston, Texas is located, "encounter[ed] between eight and ten encrypted devices every month in its criminal investigations" in 2016; the Suffolk County District Attorney's Office, in which Boston, Massachusetts is located, "encountered 151 encrypted devices" in its criminal investigations during 2016; law enforcement officials in Los Angeles, California were unable to access over 300 encrypted devices during criminal investigations in 2016; and Wisconsin's Department of Justice encountered sixty-eight encrypted devices in criminal investigations in 2016.[23]

Furthermore, the FBI was likely unable to gain access to the contents of between 1,000 and 2,000 devices that the FBI had legal authority to access in fiscal year 2017.[24] This indicates that law enforcement is encountering encryption with increasing frequency and that the problem may be quite large, especially with regards to device encryption.

B. PRIVATE SECTOR AND SECURITY CONCERNS

[21] Andy Greenberg, *Manhattan DA: iPhone Crypto Locked Out Cops 74 Times*, WIRED (July 8, 2015), http://www.wired.com/2015/07/manhattan-da-iphone-crypto-foiled-cops-74-times/.

[22] MANHATTAN DIST. ATTORNEY'S OFFICE, SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 8 (2016), http://manhattanda.org/sites/default/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

[23] *Id.* at 9–10.

[24] Devlin Barrett, *FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public*, WASH. POST (May 22, 2018), https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html?utm_term=.451c318e9ec7.

The private sector and security officials have expressed numerous reasons why they oppose a lawful access requirement for either device encryption or encryption of messages in transit.[25] The private sector and some cryptographers fear that the technological architecture that would guarantee law enforcement and intelligence agencies access would compromise user security and privacy.[26] Building in lawful access would increase systems' complexities, which would increase vulnerabilities because the new feature could interact with existing features in unintended and unknown ways.[27] Also, the keys that would need to be retained by the companies, government, or a third party would become targets for illicit actors to attack.[28] Thus, user security could be put at greater risk with a lawful access requirement for either device encryption or encryption of messages in transit. This is also very worrisome for the U.S. government because the U.S. is heavily dependent on cyber infrastructure, which makes it vulnerable to cyber-threats.[29]

In addition, surveillance by governments that have less robust legal processes than the U.S. would be made easier by the new technological architecture because U.S. products are used around the world.[30] This would conflict with America's foreign policy interests at times when strong encryption would be favored because dissidents could use it to challenge authoritarian regimes. Further, because U.S. products are used around the world, mandating lawful access for either device encryption or encryption of messages in transit would allow autocratic regimes to infringe on

---

[25] The government is not a monolithic actor in this debate, and several former national security and intelligence officials oppose a lawful access requirement.

[26] *See generally* HAROLD ABELSON ET AL., KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS (2015) (arguing against a lawful access requirement because of cybersecurity concerns).

[27] *Id.* at 15–17.

[28] *Id.*

[29] JACK GOLDSMITH & STUART RUSSELL, STRENGTHS BECOME VULNERABILITIES: HOW A DIGITAL WORLD DISADVANTAGES THE UNITED STATES IN ITS INTERNATIONAL RELATIONS 4–9 (2018).

[30] *See generally* Lu Wang, *Tech Giants Are Now Global Stock Leaders*, BLOOMBERG (Feb. 2, 2016), http://www.bloomberg.com/news/articles/2016-02-02/facebook-ascent-cements-reign-of-u-s-tech-in-global-stock-ranks (discussing how the demand for U.S. technology products around the world has spurred U.S. technology companies to become the largest companies in the world).

their citizens' privacy rights and enable these regimes to crack down on dissidents. The U.S. would not have as much leverage in condemning such actions by repressive regimes if it demanded lawful access for either device encryption or encryption of messages in transit, too, because other countries would argue that they were legitimately pursuing law enforcement and intelligence goals through their actions. On the other hand, the U.S. would be able to argue that other countries' activities and surveillance laws are overbroad and repressive. In addition, authoritarian regimes would likely be able to bypass device encryption regardless of whether lawful access for device encryption was required if they have detained the user of the device because these regimes may resort to torture to obtain the keys to the device to find the desired information.

Also, U.S. mandated lawful access for either device encryption or encryption of messages in transit would not be globally pervasive. There are 546 encrypted products from outside the U.S.[31] Thus, sophisticated illicit actors would be able to encrypt their devices or communications regardless of whether the U.S. mandated lawful access for either device encryption or encryption of messages in transit. However, many illicit actors are not sophisticated. Many criminals end up getting caught because of flawed plans or carelessness.[32] Therefore, the shift to overseas encryption products would likely not be widespread among illicit actors.

"The greatest potential harm from requiring lawful access [for either device encryption or encryption of messages in transit] likely stems from the possible decrease in the market share and economic viability of U.S. companies."[33] U.S. intelligence has had a tremendous advantage in gathering information because a great

[31] BRUCE SCHNEIER, KATHLEEN SEIDEL & SARANYA VIJAYAKUMAR, A WORLDWIDE SURVEY OF ENCRYPTION PRODUCTS 2 (2016).

[32] Alan Z. Rozenshtein, *The Encryption Debate Isn't About Stopping Terrorists, it's About Solving Crime*, LAWFARE (Apr. 9, 2018), https://www.lawfareblog.com/encryption-debate-isnt-about-stopping-terrorists-its-about-solving-crime.

[33] Eric Manpearl, *Preventing "Going Dark": A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate*, 28 U. FLA. J.L. & PUB. POL'Y 65, 82 (2017).

deal of global communications transit the U.S.[34] Following Edward Snowden's unauthorized disclosures of intelligence activities, foreign consumers have become concerned about U.S. surveillance. Foreign consumers may not want to use American products or online services if they believe their communications would be accessible to U.S. law enforcement or intelligence agencies.[35] This could decrease U.S. companies' market share, which would mean less information would be transiting U.S. networks. Thus, U.S. intelligence agencies would have a more difficult time obtaining information. Also, a decrease in U.S. companies' market share would hurt their economic viability. U.S. technology companies already lost between $35 and $180 billion in revenue over the three-year period following the Snowden disclosures.[36]

U.S. companies face a tremendous threat from the theft of intellectual property through cyber espionage. General Keith Alexander, the former Commander of U.S. Cyber Command and Director of the NSA, has stated that cyber espionage has resulted in the "greatest transfer of wealth in history."[37] U.S. companies lose

---

[34] John Markoff, *Internet Traffic Begins to Bypass the U.S.*, N.Y. TIMES (Aug. 29, 2008), http://www.nytimes.com/2008/08/30/business/30pipes.html?pagewanted=print&_r=0 (noting General Michael Hayden's, former Director of the CIA and Director of the NSA, testimony before the Senate Judiciary Committee stating that "[b]ecause of the nature of global telecommunications, we are playing with a tremendous home-field advantage, and we need to exploit that edge").

[35] *See, e.g.*, Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html (discussing the increased skepticism by foreign consumers of U.S. technology products following the Snowden disclosures).

[36] DANIEL CASTRO, HOW MUCH WILL PRISM COST THE U.S. CLOUD COMPUTING INDUSTRY? 3 (2013) (calculating that U.S. technology companies would lose up to $35 billion between 2013–2016 following Snowden's unauthorized disclosures about the NSA's intelligence programs); James Staten, *The Cost of PRISM Will Be Larger Than ITIF Projects*, FORRESTER (Aug. 14, 2013) https://go.forrester.com/blogs/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects/ (estimating that U.S. technology companies could lose up to $180 billion between 2013–2016 because of disclosures about NSA programs).

[37] Keith B. Alexander, U.S. Cyber Command Commander and NSA Director, Cybersecurity and American Power: Addressing new threats to America's

about $250 billion per year because of intellectual property theft, global cyber crime costs companies about $114 billion per year worldwide, and $388 billion is lost globally when the costs of down time are taken into account.[38] The threat of intellectual property theft and cyber crime could be exacerbated by a lawful access requirement that makes systems more vulnerable.

The decreased economic viability that could result from a lawful access requirement for either device encryption or encryption of messages in transit would diminish the U.S.'s economic strength, which is an important aspect of the U.S.'s role in the world. In 2014, Internet-related companies in the U.S. generated $966.2 billion in revenue, which accounted for 6% of real Gross Domestic Product.[39] Economic strength enables countries to have political and military power, and to have strong geopolitical influence. Therefore, it is important to consider the economic interests of U.S. businesses when considering whether a lawful access requirement for either device encryption or encryption of messages in transit is appropriate.

III. THE ENCRYPTION DEBATE OVERSEAS

The potential economic harm to U.S. companies that could result from a lawful access requirement for either device encryption or encryption of messages in transit is an extraordinarily important aspect of the encryption debate because economic strength enables countries to have political and military power, and to have strong geopolitical influence. Unfortunately, this part of the debate has been understudied thus far. In order for U.S. companies' market share and economic viability to be threatened by a lawful access requirement for either device encryption or encryption of messages in transit, companies in other nations would need to emerge and consumers—especially foreign consumers—would have to switch

economy and military (July 9, 2012), *available at* http://www.aei.org/events/cybersecurity-and-american-power/.

[38] *Id.*

[39] STEPHEN E. SIWEK, MEASURING THE U.S. INTERNET SECTOR 5 (2015).

away from American products and online services to these foreign companies based on the belief that their communications would be accessible to U.S. law enforcement or intelligence agencies if they continued to use U.S. products and services. These foreign companies would need to be unrestricted by lawful access requirements in their home countries to be able to offer consumers unbreakable encryption, which U.S. companies would no longer be able to offer if the U.S. imposed a lawful access requirement for either device encryption or encryption of messages in transit. Thus, it is important to analyze the current encryption debates in other countries and the actions being taken by other nations on this issue. This Article examines the encryption debates in France, Germany, the United Kingdom, China, and Russia to help shed light on whether there are actually viable companies and markets outside the U.S. that could threaten U.S. companies if the United States imposed a lawful access requirement for either device encryption or encryption of messages in transit.

A. FRANCE

France has suffered several terrorist attacks since 2015, which led the French government to declare a state of emergency that lasted two years and to enact security-oriented legislation.[40]

[40] Christian Hartmann, *Two Years After the Paris Attacks, France Ends State of Emergency*, REUTERS (Nov. 1, 2017), https://www.reuters.com/article/us-france-security/two-years-after-the-paris-attacks-france-ends-state-of-emergency-idUSKBN1D14KD; *see* Rukmini Callimachi, *ISIS Claims Responsibility, Calling Paris Attacks 'First of the Storm'*, N.Y. TIMES (Nov. 14, 2015), https://www.nytimes.com/2015/11/15/world/europe/isis-claims-responsibility-for-paris-attacks-calling-them-miracles.html?rref=collection%2Fnewseventcollection%2Fattacks-in-paris (discussing the Paris terrorist attacks and ISIS's involvement in the attacks); Adam Nossiter, Aurelien Breeden & Katrin Bennhold, *Three Teams of Coordinated Attackers Carried Out Assault on Paris, Officials Say; Hollande Blames ISIS*, N.Y. TIMES (Nov. 14, 2015), https://www.nytimes.com/2015/11/15/world/europe/paris-terrorist-attacks.html?rref=collection%2Fnewseventcollection%2Fattacks-in-paris (analyzing ISIS's involvement in the Paris terrorist attacks and the increased threat of external attacks from ISIS); Alissa J. Rubin & Aurelien Breeden, *ISIS Claims Truck Attacker in France Was Its 'Soldier'*, N.Y. TIMES (July 16, 2015), https://www.nytimes.com/2016/07/17/world/europe/isis-nice-france-

These terrorist attacks have been at the forefront of the French debate over whether to enact a lawful access mandate for encrypted products and services. Although French lawmakers have proposed legislation to mandate a lawful access requirement, this requirement has not yet been enacted. The French encryption debate has not distinguished between a lawful access requirement for device encryption and encryption of messages in transit.

Articles 60-1 and 60-2 of the French Criminal Procedure Code authorize French judicial police officers to obtain documents and information. Article 60-1 enables a judicial police officer to order any person "likely to possess any documents relevant to the inquiry in process" to provide the documents to the officers.[41] This provision imposes a €3,750 fine for a failure to respond to an order.[42] Article 60-2 states that people "must make available information helpful for the discovery of the truth" upon a judicial police officer's request.[43] This provision also imposes a €3,750 fine for a refusal to respond to such a request.[44] Although these provisions do not mention encryption, French authorities may be able to use these laws to demand plaintext information.[45] These Articles are analogous to—yet broader than—administrative subpoenas, grand jury subpoenas, and national security letters in U.S. law, which do not require prior judicial approval (but subpoenas and national security letters are subject to judicial review if a recipient makes a motion to modify or quash the subpoena or when judicial enforcement action occurs).[46]

---

attack.html?mcubz=0 (describing the terrorist attack in Nice and ISIS's claim of responsibility); *Nice Attack: What We Know About the Bastille Day Killings*, BBC NEWS (Aug. 19, 2016), http://www.bbc.com/news/world-europe-36801671 (recounting the public information regarding the Nice terrorist attack).

[41] CODE DE PROCÉDURE PÉNALE [C. PR. PÉN.] [CRIMINAL PROCEDURE CODE] art. L60-1 (Fr.).

[42] *Id.*

[43] *Id.* art. L60-2.

[44] *Id.*

[45] BHAIRAV ACHARYA ET AL., DECIPHERING THE EUROPEAN ENCRYPTION DEBATE: FRANCE 3 (2017).

[46] *See generally* CHARLES DOYLE, CONG. RESEARCH SERV., RS22122, ADMINISTRATIVE SUBPOENAS AND NATIONAL SECURITY LETTERS IN CRIMINAL AND INTELLIGENCE INVESTIGATIONS: A SKETCH (2005), [hereinafter DOYLE, ADMINISTRATIVE SUBPOENAS AND NATIONAL SECURITY LETTERS IN CRIMINAL

Article 230-1 of the Criminal Procedure Code empowers French authorities to appoint any person to conduct the technical operations necessary to obtain a readable version of information that has been collected pursuant to other authorities in the code and "where a method of encryption has been used, the secret key for decoding it."[47] This provision does not state the penalty for refusing to comply, and likely only applies to situations in which the person appointed by French authorities possesses the encryption key. Article 230-1 does not mandate that providers maintain encryption keys to facilitate lawful access. This provision is somewhat similar to a number of statutes in U.S. law. Article 230-1 is similar to the provision in the Communications Assistance to Law Enforcement Act (CALEA) that "[a] telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."[48] It is also somewhat analogous to the technical assistance provisions in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and the Foreign Intelligence Surveillance Act (FISA) that require providers or other specified persons to provide technical assistance necessary to accomplish the interception[49] Article 230-1 is also reminiscent of the U.S.'s All

---

AND INTELLIGENCE INVESTIGATIONS: A SKETCH]; CHARLES DOYLE, CONG. RESEARCH SERV., RL33321, ADMINISTRATIVE SUBPOENAS IN CRIMINAL INVESTIGATIONS: A BRIEF LEGAL ANALYSIS (2006), [hereinafter DOYLE, ADMINISTRATIVE SUBPOENAS IN CRIMINAL INVESTIGATIONS: A BRIEF LEGAL ANALYSIS]; CHARLES DOYLE, CONG. RESEARCH SERV., RL33320, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: LEGAL BACKGROUND (2015), [hereinafter DOYLE, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: LEGAL BACKGROUND]; U.S. DEP'T OF JUSTICE, OFFICE OF LEGAL POLICY, REPORT TO CONGRESS ON THE USE OF ADMINISTRATIVE SUBPOENA AUTHORITIES BY EXECUTIVE BRANCH AGENCIES AND ENTITIES (2002), https://www.justice.gov/archive/olp/rpt_to_congress.htm [hereinafter U.S. DEP'T OF JUSTICE, OFFICE OF LEGAL POLICY].

[47] CODE DE PROCÉDURE PÉNALE [C. PR. PÉN.] [CRIMINAL PROCEDURE CODE] art. L230-1 (Fr.).

[48] 47 U.S.C. § 1002(b)(3) (2012).

[49] *See* 18 U.S.C. § 2518(4) (2012) (requiring that upon court order "a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a

Writs Act, which has come to be understood as authorizing a federal court to issue a writ directing a third-party to an underlying litigation to provide reasonable technical assistance to the government to facilitate the execution of a valid search warrant in the aftermath of the U.S. Supreme Court's decision in *New York Telephone Co.* in 1977.[50]

Article 434-15-2 of the French Penal Code states that "anyone who, having a key to decipher an encrypted message which may have been used to prepare, facilitate or commit a felony or a misdemeanor, refuses to disclose that key to the judicial authorities or to operate it following instructions by the judicial authorities" faces a penalty of three years in prison and a €270,000 fine.[51] This Article increases the penalty to five years in prison and a €450,000 fine if the refusal to disclose the encryption key or operate it "would have prevented the commission of a felony or a misdemeanor or would have limited its consequences."[52] France thus has the ability to punish people who possess encryption keys but refuse to comply with lawful orders to disclose or operate those keys with severe financial penalties and jail sentences, but does not have an explicit lawful access requirement to mandate that technology companies

---

minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted"); 50 U.S.C. § 1805(c)(2)(B) (2012) (stating that the Foreign Intelligence Surveillance Court (FISC) shall direct that "upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person . . . furnish the applicant 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 with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance").

[50] 28 U.S.C. § 1651 (2012); United States v. New York Tel. Co., 434 U.S. 159, 172–75 (1977); *see* In re Apple, Inc., 149 F. Supp. 3d 341, 364–73 (E.D.N.Y. 2016) (denying order that would require Apple to technically assist in the execution of a search warrant previously issued by the court); *see also* Robert Chesney & Steve Vladeck, *A Coherent Middle Ground in the Apple-FBI All Writs Act Dispute?*, LAWFARE (Mar. 21, 2016), https://www.lawfareblog.com/coherent-middle-ground-apple-fbi-all-writs-act-dispute (arguing that "the All Writs Act should be read to authorize the…order the government has sought…only when the recipient is compelled to help the government utilize existing vulnerabilities in its software").

[51] CODE PENAL [C. PÉN.] [PENAL CODE] art. L434-15-2 (Fr.).

[52] *Id.*

maintain the ability to provide plaintext information upon lawful process.

Article 434-15-2 is similar to CALEA, FISA and Title III's technical assistance provisions, and the All Writs Act in U.S. law, but these provisions in U.S. law do not have such severe enforcement provisions.[53] Article 434-15-2 is also similar to contempt charges in the United States for failure to comply with a court order, but the United States may provide additional protections in certain circumstances under the Fifth Amendment. The Fifth Amendment privilege protects an individual from being "compelled in any criminal case to be a witness against himself."[54] The Supreme Court has interpreted this as protecting an individual from being compelled to give testimony that is self-incriminating.[55] Cases typically focus on whether a statement is testimonial, as compulsion and the incriminating nature of documents are rarely in doubt. The Supreme Court has held that it is testimony implicating the Fifth Amendment when the government compels an individual to use the contents of his own mind to communicate a fact or disclose information.[56] The Eleventh Circuit Court of Appeals in *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011* ruled that compelled password decryption violates the Fifth Amendment because it involves requiring the defendant to use the defendant's mind to incriminate himself unless the government can demonstrate that the existence of the information sought is a "foregone conclusion" by demonstrating that it knows with "reasonably particularity" that the device contained the sought-after material.[57] However, the Third Circuit Court of Appeals in *U.S. v. Apple MacPro Computer* in 2017, included a footnote hinting that the proper analysis under the "foregone conclusion" doctrine is solely whether the government can show with "reasonably particularity" that it knows that the person knows the password.[58] At least one

[53] 18 U.S.C. § 2518(4) (2012); 28 U.S.C. § 1651 (2012); 47 U.S.C. § 1002(b)(3) (2012); 50 U.S.C. § 1805(c)(2)(B) (2012).
[54] U.S. Const. amend. V.
[55] Fisher v. United States, 425 U.S. 391, 409–11 (1976).
[56] Doe v. United States, 487 U.S. 201, 210–11 (1988).
[57] United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1346–49 (11th Cir. 2012).
[58] United States v. Apple MacPro Computer, 851 F.3d 238, 248 n.7 (3d Cir. 2017).

district court has followed the Third Circuit's lead and only examined whether the government can show that it is a "foregone conclusion" that the person knows the password.[59]

Further, France amended its surveillance law in July 2015. Article 871-1 of the French Code of Internal Security requires that entities that provide encryption for confidentiality purposes must provide the information required to decrypt the data to authorities within 72 hours of an authorized request for the information.[60] Failure to comply with this requirement is punishable by two years in jail and a €150,000 fine.[61] However, entities that can demonstrate that they are unable to comply with requests are relieved of the responsibilities under Article 871-1, which likely means that technology companies that do not possess the capability to decrypt user data are not subject to this provision and would not face the punishments for failing to comply with this law. This provision is also similar to CALEA, FISA and Title III's technical assistance provisions, and the All Writs Act in U.S. law.[62]

The primary legislative debates regarding encryption in France occurred in 2016. In January 2016, just two months after the November 13, 2015 terrorist attacks in Paris, Deputy Nathalie Kosciusko-Morizet, a senior member of the conservative Les Républicains Party, introduced an amendment on encryption to the bill that would become the Digital Republic Law, which updated France's legal regime on net neutrality rules, data privacy rules, and aspects of the digital economy.[63] Kosciusko-Morizet's proposed amendment stated that "[e]quipment manufacturers must take into account in their constructions the need to give law enforcement, in the context of a judicial inquiry and after authorization of a judge, access to the material."[64] The proposal would have authorized the

[59] United States v. Spencer, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018).
[60] CODE DE LA SÉCURITÉ INTÉRIEURE [C. SEC. INT.] [CODE OF INTERNAL SECURITY] art. L871-1 (Fr.).
[61] *Id.* art. L881-2.
[62] 18 U.S.C. § 2518(4) (2012); 28 U.S.C. § 1651 (2012); 47 U.S.C. § 1002(b)(3) (2012); 50 U.S.C. § 1805(c)(2)(B) (2012).
[63] DANIEL SEVERSON, THE ENCRYPTION DEBATE IN EUROPE 2 (2017).
[64] Nathalie Kosciusko-Morizet et al., *Amendement nºCL92 to République Numérique nº3318*, ASSEMBLÉ NATIONALE (Jan. 4, 2016), http://www.assemblee-nationale.fr/14/amendements/3318/CION_LOIS/CL92.asp.

Council of the State, which is a government entity that serves as a legal adviser to the executive branch, to develop the detailed rules for the application of the proposal.[65] Kosciusko-Morizet intended for her proposal to "open the debate on ways and means to ensure access to data for reasons of national security and in the context of a judicial inquiry."[66] The proposal's summary recognized that while the increased prevalence of encryption enhances protection for user data, it also impairs the government's ability to provide security for the nation.[67] However, Axelle Lemaire, then-Minister of Digital Affairs and member of the Socialist Party, which held the presidency and formed the government in 2016, argued that the proposal was a "vulnerability by design" and should be rejected.[68] Lamaire stressed that a lawful access requirement would decrease users' security and would result in illicit actors being able to exploit vulnerabilities created by such a regime.[69] Also, Lemaire stated that a lawful access requirement would lead to economic harm for technology companies because they would suffer reputational harm from being seen as having less secure products and services.[70] Kosciusko-Morizet ultimately withdrew her amendment as the government's opposition to it hindered its prospects of being passed.[71]

The encryption debate returned to the forefront several months later during debates over the Organized Crime and Terrorism Act of 2016, which occurred at the same time that the FBI and Apple dispute over whether Apple could be compelled to unlock the iPhone of one of the San Bernardino terrorists played out in the

[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] Guillaume Champeau, *Chiffrement: Le Gouvernement Rejettee Les Backdoors*, NUMERAMA (Jan. 13, 2016), https://www.numerama.com/politique/138689-chiffrement-le-gouvernement-rejette-les-backdoors.html; Glyn Moody, *French Government Rejects Crypto Backdoors as "The Wrong Solution"*, ARS TECHNICA (Jan. 14, 2016), https://arstechnica.com/tech-policy/2016/01/french-government-rejects-crypto-backdoors-as-the-wrong-solution/.
[69] Moody, *supra* note 68.
[70] *Id.*
[71] Champeau, *supra* note 68.

United States.[72] Deputy Philippe Goujan, a member of Les Républicains Party, proposed an amendment to the counterterrorism bill to modify Articles 60-1, 60-2, and 230-1 of the Criminal Procedure Code.[73] Goujan's proposal would have increased the fine imposed for a failure to respond to an order under Article 60-1 from €3,750 to €15,000 and imposed a penalty of two years in prison when the request for information was related to terrorism investigations.[74] Similarly, the proposal would have increased the fine imposed for a refusal to respond to a request under Article 60-2 from €3,750 to €15,000 and imposed a penalty of two years in prison when the request for information was related to terrorism investigations.[75] Further, the proposal would have added provisions to Articles 60-2 and 230-1 to impose a €350,000 fine and five-year imprisonment on private companies and the companies' executives that refused to communicate decrypted data to a requesting judicial authority investigating terrorism offenses when the company was responsible for the data being encrypted.[76] Deputy Goujon argued that the current penalties in French law were insufficient to force technology companies to comply with lawful orders to obtain encrypted information and hoped the more robust punishments would incentivize companies to comply with French authorities.[77] Deputy Eric Ciotti, who was a co-sponsor of the amendment and also a member of Les Républicains Party, defended the proposal by stating that France needed to take action against the "giant" multinational technology companies based in Silicon Valley that "refuse to cooperate with justice."[78] This amendment was ultimately

[72] *See* Eric Lichtblau & Kate Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html (describing the FBI and Apple dispute).

[73] Philippe Goujan et al., *Amendement nº90 to Lutte Contre le Crime Organisé, le Terrorisme et Leur Financement nº3515*, ASSEMBLÉ NATIONALE (Feb. 23, 2016), http://www.assemblee-nationale.fr/14/amendements/3515/AN/90.asp.

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *Assemblée Nationale XIV Législature Session Ordinaire de 2015–2016, Deuxié Séance du Jeudi 03 Mars 2016*, *ASSEMBLÉE NATIONALE* (Mar. 3, 2016), http://www.assemblee-nationale.fr/14/cri/2015-2016/20160141.asp#P738130.

[78] *Id.*

adopted by the National Assembly.[79] However, the Senate stripped Deputy Goujon's proposal from the final legislation.[80] The Senate Committee of Laws determined that the proposal's significant penalties of a €350,000 fine and possible five-year jail sentence for companies and executives that refused to communicate decrypted data in terrorism investigations was "superfluous and counterproductive" so the Committee stripped this provision from the final bill.[81] Specifically, the Senate Committee of Laws determined that the proposal would add confusion to the legal framework in this area because Article 434-15-2 of the Penal Code imposes fines and possible jail time for those who have encryption keys that can decrypt a message that may have been part of a criminal activity, but refuse to disclose the keys to judicial authorities.[82] The provision's amendments of Articles 60-1 and 60-2 of the Criminal Procedure Code to increase the fines and impose jail time for a failure or refusal to comply with these laws were also removed by the Senate.[83] The Senate did significantly increase the financial penalties imposed by Article 434-15-2 of the Penal Code to the amounts stated *supra*, though. Prior to the Organized Crime and Terrorism Act of 2016, Article 434-15-2 only imposed a €45,000 fine on anyone who had the key to decrypt messages that may have been part of criminal activity, but refused to disclose the

[79] *Id.*

[80] *See* Loi 2016-1321 du 7 octobre 2016 pour une République numérique [Law 2016-1321 of October 7, 2016 for a Digital Republic], Journal Officiel de la République Francaise [J.O.] [Official Gazette of France], Oct. 8, 2016 (not including Deputy Goujon's proposal in the final statute).

[81] *Projet de Loi Renforçant la Lutte Contre le Crime Organisé, le Terrorisme et Leur Financement, et Améliorant L'efficacité et Les Garanties de la Procédure Pénale*, SÉNAT, http://www.senat.fr/rap/l15-491-1/l15-491-17.html#toc75.

[82] *Id.*; Daniel Severson, *Encryption Legislation Advances in France*, LAWFARE (Apr. 14, 2016), https://www.lawfareblog.com/encryption-legislation-advances-france.

[83] *See* Loi 2016-1321 du 7 octobre 2016 pour une République numérique [Law 2016-1321 of October 7, 2016 for a Digital Republic], Journal Officiel de la République Francaise [J.O.] [Official Gazette of France], Oct. 8, 2016 (not including this proposal in the final statute).

key to judicial authorities, and a €75,000 fine if cooperation would have prevented a crime or diminished its effects.[84]

Also, Deputy Ciotti proposed an amendment to the bill in the National Assembly to add a provision to the Penal Code to require "manufacturers of telecommunications tools, telecommunications operators, [and] Internet service providers" to "provide all information relevant" as part of a terrorist investigation to French authorities.[85] This proposal stated that violators of the obligation would be subject to a fine of up to €2 million and up to a one-year ban from the French market for the products and services of any company that did not comply.[86] Deputy Ciotti argued that French authorities were increasingly encountering encrypted devices and alleged that the November 2015 terrorist attacks could have been thwarted if not for encryption.[87] He also defended the harsh penalties in his proposal by stating that such extreme measures were necessary "in the face of companies with market capitalization of several hundred billion dollars, which consider states as dwarves and disregard laws and rules."[88] Thus, Deputy Ciotti sought to rally support behind his proposal by inspiring nationalistic sentiments that he was leading a charge on behalf of French freedom and security against multinational companies based overseas "to signal to these companies that their financial rules will never be superior to the laws of a democratic state."[89] Other members of the National Assembly pushed back against such a severe approach and Deputy Sergio Coronado of the Greens Party argued that companies were not solely motivated by financial interests and immune to concerns over terrorism.[90] Deputy Coronado argued that encryption enhanced

[84] Loi 2001-1062 du 15 novembre 2001 relative á le sécurité quotidienne [Law 2001-1062 of November 15, 2001 on Daily Security], Journal Officiel de la République Francaise [J.O.] [Official Gazette of France], Nov. 16, 2001, art. 31.
[85] Eric Ciotti et al., *Amendement nº221 to Lutte Contre le Crime Organisé, le Terrorisme et Leur Financement nº3515*, ASSEMBLÉ NATIONALE (Feb. 25, 2016), http://www.assemblee-nationale.fr/14/amendements/3515/AN/221.asp.
[86] *Id.*
[87] *Assemblée Nationale XIV Législature Session Ordinaire de 2015–2016, Premiére Séance du Jeudi 03 Mars 2016*, ASSEMBLÉE NATIONALE (Mar. 3, 2016), http://www.assemblee-nationale.fr/14/cri/2015-2016/20160140.asp.
[88] *Id.*
[89] *Id.*
[90] *Id.*

privacy protections and that parliamentarians should consider what would happen if authoritarian regimes were able to obtain decryption keys from companies.[91]

Further, Deputy Yann Galut of the Socialist Party offered two amendments that were focused on encryption. Both proposals authorized authorities to "require the designer of electronic equipment to access, by any means, data likely to be of interest to the current investigations contained in electronics of its design," and imposed a €1 million fine for a refusal to answer such requests.[92] Deputy Galut echoed the concerns of other parliamentarians over the increased prevalence of authorities not being able to access smartphones related to criminal or terrorism investigations because of encryption.[93] Deputy Galut also attacked "multinationals [that] have decided to enact their own law," and called on his fellow lawmakers to protect victims and constrain these companies' actions on encryption.[94] Deputy Pascal Popelin of the Socialist Party joined Deputy Galut in calling on lawmakers to find a solution to resolve the difficulties presented by unbreakable encryption, and stated that France should "no longer be confronted with this kind of blocking in the name of a pseudo-defense of freedom."[95]

Jean-Jacques Urvoas, then-Minister of Justice, expressed the government's view that the issue needed to be dealt with at the international level, or at least the European level, and that a national law was not the best way to proceed at the time.[96] Minister Urvoas thus asked Deputy Galut and Deputy Ciotti to withdraw their

---

[91] *Id.*
[92] Yann Galut et al., *Amendement nº532 to Lutte Contre le Crime Organisé, le Terrorisme et Leur Financement nº3515*, ASSEMBLÉ NATIONALE (Feb. 29, 2016), http://www.assemblee-nationale.fr/14/amendements/3515/AN/532.asp; Yann Galut et al., *Amendement nº533 to Lutte Contre le Crime Organisé, le Terrorisme et Leur Financement nº3515*, ASSEMBLÉ NATIONALE (Feb. 29, 2016), http://www.assemblee-nationale.fr/14/amendements/3515/AN/533.asp.
[93] *Assemblée Nationale XIV Législature Session Ordinaire de 2015–2016, Premiére Séance du Jeudi 03 Mars 2016*, ASSEMBLÉE NATIONALE (Mar. 3, 2016), http://www.assemblee-nationale.fr/14/cri/2015-2016/20160140.asp.
[94] *Id.*
[95] *Id.*
[96] *Id.*

proposals.[97] While Deputy Galut agreed to withdraw his proposals, Deputy Ciotti refused.[98] Ultimately, Deputy Ciotti's proposal was defeated by one vote in the National Assembly.[99]

Although France did not pass a lawful access requirement during the intense legislative debates that occurred in 2016, the encryption debate has continued. In August 2016, French Interior Minister Bernard Cazeneuve stated that he planned to work with his German counterpart, Thomas de Maizière, the country's Federal Minister of the Interior, to promote an international initiative to regulate encryption.[100] France and Germany had both suffered several terrorist attacks and authorities openly discussed that terrorist groups were utilizing encryption technologies.[101] This led Cazenuve and de Maizière to hold a joint press conference in Paris to call on the "European Commission to change the law to afford security agencies the ability to access encrypted data."[102] In February 2017, the new French Interior Minister, Bruno Le Roux, and de Maizière sent a letter to the European Commission calling for various security proposals to be enacted to combat the terrorist threat in Europe, which included advocating for a lawful access requirement.[103] The EU Commissioner, Věra Jourová, concurred with the French and German ministers concerns and stated that the

---

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] Reuters, *France and Germany Want to Stop Islamic Extremists From Using Messaging Encryption*, FORTUNE (Aug. 11, 2016), http://fortune.com/2016/08/11/france-messaging-encryption/.

[101] Sam Jones et al., *EU Spymasters Lobby for Change in Encryption Law*, FIN. TIMES (Aug. 22, 2016), https://www.ft.com/content/08fe566e-679e-11e6-ae5b-a7cc5dd5a28c.

[102] Natasha Lomas, *Encryption Under Fire in Europe as France and Germany Call for Decrypt Law*, TECH CRUNCH (Aug. 24, 2016), https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/.

[103] Letter from Thomas de Maizière & Bruno Le Roux to Frans Timmermans, POLITICO (Feb. 20, 2017), http://www.politico.eu/wp-content/uploads/2017/02/2017-02-17-De%CC%81claration-FR-DE-II_Officielle.pdf; Iain Thomson, *Germany, France Lobby Hard for Terror-Busting Encryption Backdoors–Europe Seems to Agree*, THE REGISTER (Feb. 28, 2017), https://www.theregister.co.uk/2017/02/28/german_french_ministers_breaking_encryption/.

European Commission would consider legislative and other options to enable law enforcement and intelligence authorities to gain access to plaintext information.[104]

Thus far, the European Commission has not moved forward with a lawful access requirement for either device encryption or encryption of messages in transit. Instead, the European Commission announced a series of measures in October 2017 to support law enforcement authorities in member states.[105] The Commission will increase the number of personnel at Europol focused on developing decryption capabilities and study whether Europol needs more financial resources to address the issue, support law enforcement agencies at the national level in establishing networks of technical experts and facilitate collaboration between these national groups of experts, train law enforcement on methods of obtaining information that is stored on encrypted devices and plaintext communications, set up forums to facilitate collaboration between governments and service providers, and continue to study the impact that encryption technologies have on criminal investigations.[106] In addition, the European Commission called on authorities in member states to develop a "toolbox of alternative investigation techniques" to facilitate obtaining plaintext information, which likely refers to lawful hacking, and stated that Europol would be a good repository for these "techniques and tools."[107]

Encryption also became part of France's 2017 presidential election and Emmanual Macron stated that he would increase efforts to obtain plaintext information from technology companies that offer encryption. In April 2017, Macron declared that "[i]f I am elected, France will launch a major initiative beginning this summer

---

[104] Catherine Stupp, *EU to Propose New Rules Targeting Encrypted Apps in June*, EURACTIV (Mar. 28, 2017), https://www.euractiv.com/section/data-protection/news/eu-to-propose-new-rules-on-police-access-to-encrypted-data-in-june/.

[105] *Communication from the Commission to the European Parliament, The European Council and the Council: Eleventh Progress Report Towards an Effective and Genuine Security Union*, at 8–10, COM (2017) 608 final (Oct. 18, 2017).

[106] *Id.*

[107] *Id.* at 9–10.

targeting the major Internet providers, so that they agree to the legal seizure of data from their encrypted services as part of the fight against terrorism."[108] Macron was subsequently elected President and issued a proposal with UK Prime Minister Theresa May in June 2017 to combat terrorist activities on the Internet, which in part called for authorities to have access to the plaintext content of communications and metadata in criminal and terrorist investigations.[109] The encryption debate in France has been rather quiet since this announcement, and the Macron government has not pushed for new national legislation in France.

Overall, the French encryption debate has largely focused on terrorists' use of encryption technologies and the threat that France faces from terrorism, especially in the aftermath of a spate of terrorist attacks over the last few years. Proponents of a lawful access mandate have cited these terrorism concerns, and have also sought to vilify large multinational technology companies in their efforts to gain support for proposals that regulate encryption. Many of the debates surrounding the various legislative proposals in 2016 specifically focused on U.S.-based multinational technology companies and sought to portray these companies as being unconcerned with French security. Several of these proposals came very close to being enacted into law in 2016 and President Macron has called for authorities to have access to plaintext information. This indicates that France may once again attempt to pass a lawful access requirement, especially if France's efforts for more robust action at the EU-level are not successful or France suffers another terrorist attack. The opposition to a lawful access requirement in France seems to be largely focused on the concern that this requirement could diminish cybersecurity overall. Individuals on this side of the debate fear that user's will be less secure from illicit actors if they do not have access to unbreakable encryption, and

---

[108] Sébastian Seibt, *French Candidate Macron Targets Encryption in Fight Against Terrorism*, FR. 24 (Apr. 13, 2017), http://www.france24.com/en/20170412-candidate-macron-encryption-fight-terror-whatsapp-telegram.

[109] *Utilisation de L'Internet* à *des Fins Terroristes: Plan D'actions Franco-Britannique*, MINISTÈRE DE L'INTÉRIEUR (June 14, 2017), https://www.interieur.gouv.fr/Le-ministre/Communiques/Utilisation-de-l-Internet-a-des-fins-terroristes-plan-d-actions-franco-britannique.

believe that this concern outweighs the potential security benefits of a lawful access requirement.

Finally, the fact that France's debate is largely focused on U.S.-based technology companies indicates that France does not have a strong technology industry of its own that could take away market share from U.S.-based companies if the U.S. were to enact a lawful access requirement for either device encryption or encryption of messages in transit. American technology products seem to dominate the French market, too, and there do not seem to be other technology companies that would vastly increase their market share in France as a result of an American lawful access requirement for either device encryption or encryption of messages in transit. Google's Android operating system has about 61% market share of the mobile operating system market and Apple's iOS has about 38% market share of the mobile operating system market in France as of 2018.[110] U.S.-based technology companies also dominate the social media market in France as Facebook possesses about 76% of the market share, YouTube possesses about 2% of the market share, and Twitter possesses about 4% of the market share in France as of February 2019.[111] Further, Google Chrome has about 58% of the browser market share in France, Apple's Safari has about 19% of the browser market share in France, Mozilla's Firefox has about 9% of the browser market share in France, and Google has about 94% of the search engine market share in France as of February 2019.[112] Thus, U.S. technology products and services seem to control the French market and there do not seem to be other major technology companies that would readily replace these companies' market share in France if the U.S. enacted a lawful access requirement for either device encryption or encryption of messages in transit. Further, given France's own robust debate on enacting a lawful access

[110] *Mobile Share of Mobile Operating Systems in France from 2010 to 2018*, STATISTA, https://www.statista.com/statistics/639990/market-share-mobile-operating-systems-france/ (last visited Mar. 28, 2019).

[111] *Social Media Stats France*, STAT COUNTER, http://gs.statcounter.com/social-media-stats/all/france (last visited Mar. 28, 2019).

[112] *Browser Market Share France*, STAT COUNTER, http://gs.statcounter.com/browser-market-share/all/france (last visited Mar. 28, 2019); *Search Engine Market Share France*, STAT COUNTER, http://gs.statcounter.com/search-engine-market-share/all/france (last visited Mar. 28, 2019).

requirement and the possibility that the Macron government will push for such measures, it seems unlikely that U.S. products and services would suffer grave reputational harms among French consumers if the U.S. enacted a lawful access requirement for either device encryption or encryption of messages in transit, and unlikely that U.S.-based companies that produce encrypted communications applications would relocate to France as a result of a U.S. lawful access mandate for encryption of messages in transit.

B. GERMANY

Although Thomas de Maizière, Germany's Federal Minister of the Interior, joined France's ministers of interior in calling on the European Commission to enact a lawful access requirement at the EU level, Germany has largely embraced encryption thus far. Germany has instead focused on establishing a lawful hacking legal regime to obtain communications that are applicable to investigative activities.

In 1991, Germany split its cryptography unit from the Federal Intelligence Service (Bundesnachrichtendienst (BND)) to form a new civilian agency called the Federal Office for Information Security (Bundesamtes für Sicherheit in der Informationstechnik (BSI)), which is subordinate to the Ministry of the Interior (Bundesministerium des Innern (BMI)).[113] The BSI was charged with promoting secure information technology.[114] The German government subsequently adopted an encryption policy in 1999 to promote user security through secure encryption products and stressed that "in Germany encryption methods and products may continue to be developed, manufactured, marketed and used without

[113] Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik [BSIG] [BSI Establishment Act], Dec. 17, 1990, BUNDESGESETZBLATT, Teil I [BGBL I] at 2834 (Ger.); Sven Herpig & Stefan Huemann, *Germany's Crypto Past and Hacking Future*, LAWFARE (Apr. 13, 2017), https://www.lawfareblog.com/germanys-crypto-past-and-hacking-future.

[114] Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik [BSIG] [BSI Establishment Act], Dec. 17, 1990, BGBL I at 2834, § 3 (Ger.).

restriction."[115] The policy laid out five key tenets, which German officials have stated continue to guide the government's encryption policy:

> 1. There will be no ban or limitation on crypto products[.]
>
> 2. Crypto products shall be tested for their security in order to increase the user's trust in those products[.]
>
> 3. The development of crypto products by German manufacturers is essential for the country's security and their ability to compete internationally shall therefore be strengthened[.]
>
> 4. Law enforcement and security agencies shall not be weakened by the widespread use of encryption. The development of additional technical competencies for those agencies shall be fostered[.]
>
> 5. International cooperation on crypto issues such as open standards and interoperability is vital and shall be fostered bi- and multilaterally[.][116]

The German government continued its strong support for encryption technologies in its Digital Agenda 2014–2017. The policy paper stated that Germany aimed to be the world's leading country in encryption technologies and called for the widespread adoption of encryption for private communications.[117] Numerous German

---

[115] Pressemitteilung des Bundesministerium des Innern & Bundesministerium für Wirtschaft un Technologie [Press Release of the Federal Ministry of the Interior and Federal Ministry of Economics and Technology], *Eckpunkte der Deutschen Kryptopolitik*, DIE RAVEN (June 2, 1999), https://hp.kairaven.de/law/eckwertkrypto.html.

[116] Herpig & Huemann, *supra* note 113; *see also Eckpunkte der Deutschen Kryptopolitik*, *supra* note 115.

[117] FEDERAL MINISTRY FOR ECONOMIC AFFAIRS AND ENERGY, DIGITAL AGENDA 2014–2017 31 (2014), https://web.archive.org/web/20170519011016/https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda-

government officials subsequently signed a 2015 Charter to Strengthen Trustworthy Communication to promote end-to-end encryption as a way to fulfill the aspirations set forth in the Digital Agenda 2014–2017.[118]

As encryption technologies have become more prevalent, German law enforcement and intelligence agencies have focused on lawful hacking to obtain the necessary information for their investigations rather than pushing for any type of lawful access requirement.[119] German authorities began exploiting vulnerabilities to facilitate investigatory searches in the early 2000s, and this sparked substantial legal and political debate.[120] In 2006, the German state of North-Rhine Westphalia passed a statute that provided the clearest authority to date for authorities to exploit vulnerabilities to conduct online searches. Specifically, the North-Rhine Westphalia Constitutional Protection Act authorized the "secret monitoring and other reconnaissance of the Internet, such as in particular concealed participation in its communication facilities and searching therefor, as well as secret access to information technology systems also involving the deployment of technical means."[121] In 2007, federal authorities, led by the BMI, openly contemplated engaging in these techniques targeted at terror suspects.[122] Critics worried about the privacy intrusion of exploiting vulnerabilities and questioned how widespread such techniques would become.[123] The North-Rhine Westphalia Constitutional Protection Act was challenged in court and the Federal

---

engl.pdf;jsessionid=F3B2ACAE685B3BA1E51872701E135636.s5t1?__blob=publicationFile&v=6 [hereinafter GERMAN DIGITAL AGENDA 2014–2017].

[118] CHARTA ZUR STÄRKUNG DER VERTRAUENSWÜRDIGEN KOMMUNIKATION [CHARTER TO STRENGTHEN TRUSTWORTHY COMMUNICATION] 1–2 (2015), https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/2015/charta-vertrauenswuerdige-kommunikation.pdf?__blob=publicationFile.

[119] BHAIRAV ACHARYA ET AL., DECIPHERING THE EUROPEAN ENCRYPTION DEBATE: GERMANY 6 (2017).

[120] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Feb. 27, 2008, 120 ENTSCHEIDUNGEN DES BUNDESVERFASSUNGERICHTS [BVERFGE] 274 (277–78), 2008 (Ger.).

[121] *Id.* at 282.

[122] *Berlin's Trojan: Debate Erupts Over Computer Spying*, DER SPIEGEL (Aug. 30, 2007), http://www.spiegel.de/international/germany/berlin-s-trojan-debate-erupts-over-computer-spying-a-502955.html.

[123] *Id.*

Constitutional Court greatly constrained law enforcement's hacking operations in its 2008 decision striking down the Act's authorization to conduct hacking operations.[124] The Court determined that the Act's authorization for exploiting vulnerabilities encroached on Germany's general right of personality, which includes the "fundamental right to the guarantee of the confidentiality and integrity of information technology systems."[125] Exploiting vulnerabilities to access communications and stored content could only be constitutionally permissible if a concrete danger to an important legal interest existed.[126] The Court listed "life, limb and freedom of the individual or such interests of the public a threat to which affects the basis or continued existence of the state or the basis of human existence" as predominantly important legal interests that could justify hacking operations.[127] Further, the Court required authorities to get permission from a neutral body, such as a judge, prior to using such techniques and stated that authorities could not collect personal data during the course of the investigation.[128] This decision required German law enforcement agencies to develop a more tailored approach to lawful hacking.

Germany amended its Federal Criminal Police Office Act in 2008 to increase the Federal Criminal Police Office's (Bundeskriminalamt (BKA)) investigatory powers in an effort to combat terrorism.[129] This legislation included an authorization to use hacking operations to obtain evidence in terrorism investigations.[130] The legislation was criticized by some for solidifying too much power in the federal police instead of relying on state police forces, not granting parliament enough oversight, and infringing on people's private lives.[131] This law was challenged and

[124] 120 BVERFGE 274 (Ger.).
[125] *Id.* at 303.
[126] *Id.* at 274.
[127] *Id.*
[128] *Id.* at 332–33.
[129] Gesetz zur Abwehr von Gerahren des Internationalen Terrorismus Durch das Bundeskriminalamt [BKATerrAbwG] [Law on the Prevention of Threats of International Terrorism by the Federal Criminal Police Office], Dec. 25, 2008, BUNDESGESETZBLATT, Teil I [BGBL I] at 3083 (Ger.).
[130] *See id.* § 20k.
[131] *Big Brother Worries: German Parliament Passes Anti-Terror Law*, DER SPIEGEL (Nov. 13, 2008), http://www.spiegel.de/international/germany/big-

in 2016, the Federal Constitutional Court determined that numerous provisions, including the authorization for the use of hacking techniques, were inconsistent with the Constitution.[132] The Court found that the law's hacking and other surveillance authorizations were overly broad, lacked sufficiently independent oversight, and did not provide sufficient protections for the "core area of private life," such as restrictions on the use of information collected and minimization of information collected.[133] These provisions were allowed to remain in effect until June 2018, though, because the Court held that the core powers granted in these provisions did not offend the Constitution—Germany must amend these authorities to include greater restrictions to continue to use these investigatory powers.[134]

Law enforcement has been heavily reliant upon hacking operations as the terrorist threat continues to grow in Germany and more data becomes encrypted. De Maizière's calls alongside France's Ministers of Interior in 2016 and early 2017 for the European Commission to enact a lawful access requirement at the EU level gave some indication that at least part of the German government believed that this was perhaps a better approach moving forward to law enforcement's difficulties with encryption than lawful hacking.[135] However, in June 2017, Germany passed an amendment to its criminal code, which included provisions to authorize law enforcement to conduct hacking operations to gather evidence regarding a broad array of crimes, and this new law went into effect in August 2017.[136] German authorities must obtain a

---

brother-worries-german-parliament-passes-anti-terror-law-a-590198.html; Harold Neuber, *Schritt zu Einem Deutschen FBI und zum Präventionsstaat*, TELEPOLIS (Nov. 13, 2008), https://www.heise.de/tp/features/Schritt-zu-einem-deutschen-FBI-und-zum-Praeventionsstaat-3420765.html.

[132] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Apr. 29, 2016, 141 ENTSCHEIDUNGEN DES BUNDESVERFASSUNGERICHTS [BVERFGE] 220 (222), 2016 (Ger.).

[133] *Id.* at 303–16.

[134] *Id.* at 351–52.

[135] *See* Letter from Thomas de Maizière & Bruno Le Roux to Frans Timmermans, *supra* note 103.

[136] Gesetz zur Effektiveren und Praxistauglicheren Ausgestaltung des Strafverfahrens [Act to Make Criminal Proceedings More Effective and Practicable], Aug. 23, 2017, BUNDESGESETZBLATT, Teil I [BGBL I] at 3202 (Ger.); Jenny Gesley, *Germany: Expanded Telecommunications Surveillance and*

court order before engaging in hacking operations under this authority unless there is imminent danger.[137] The goal of these new provisions was to enable law enforcement to gain access to plaintext data on a suspect's device by exploiting vulnerabilities because law enforcement has been increasingly unable to obtain such information through other surveillance methods with the increased prevalence of end-to-end encryption.[138]

These provisions have been criticized for the procedure in which they were added to the legislation and for infringing upon people's privacy. The provisions were added to the legislation as an addendum to an unrelated bill, which caused members of the Green Party, who opposed the bill, and the German Lawyers Association to argue that the process lacked transparency and was undemocratic because it did not provide for sufficient debate on the issue.[139] Further, numerous privacy and civil liberties groups joined the Green Party in arguing that the law is overly intrusive into individual's privacy rights and violates the German Constitution's protections of fundamental rights.[140] In addition, the Chaos Computer Club, a European association of hackers that is based in Germany, alleged that the government's exploitation of vulnerabilities to investigate ordinary criminal activity would result

Online Search Powers, LIBR. OF CONGRESS (Sept. 7, 2017), http://www.loc.gov/law/foreign-news/article/germany-expanded-telecommunications-surveillance-and-online-search-powers/.

[137] Gesetz zur Effektiveren und Praxistauglicheren Ausgestaltung des Strafverfahrens [Act to Make Criminal Proceedings More Effective and Practicable], Aug. 23, 2017, BGBL I at 3206 (Ger.).

[138] Victor Brechenmacher, *German Government to Spy on Encrypted Messaging Services*, POLITICO (June 22, 2017), https://www.politico.eu/article/german-government-to-spy-on-encrypted-messaging-services/.

[139] Carla Bleiker, *New Surveillance Law: German Police Allowed to Hack Smartphones*, DEUTSCHE WELLE (June 22, 2017), http://www.dw.com/en/new-surveillance-law-german-police-allowed-to-hack-smartphones/a-39372085; DAV Gegen Einführung der Online-Durchsuchung und Quellen-TKÜ, DEUTSCHER ANWALT VEREIN (June 19, 2017), https://anwaltverein.de/de/newsroom/pm-7-17-dav-gegen-einfuehrung-der-online-durchsuchung-und-quellen-tkue.

[140] Andre Meister, *Staatstrojaner: Bundestag hat das Krasseste Überwachungsgesetz de Legislaturperiode Beschlossen*, NETZPOLITIK (June 19, 2017), https://netzpolitik.org/2017/staatstrojaner-bundestag-beschliesst-diese-woche-das-krasseste-ueberwachungsgesetz-der-legislaturperiode/.

in diminished cybersecurity for society as a whole.[141] Members of the governing coalition—the Christian Democratic Union of Germany (CDU), Christian Social Union in Bavaria (CSU), and Social Democrats (SPD)—that passed the law argued that it was necessary to circumvent encryption and modernize law enforcement's ability to investigate criminals and terrorists, who are increasingly communicating online rather than over phone calls, and using encrypted products and services.[142] This new legislation likely firmly cements Germany's approach to the encryption debate as engaging in lawful hacking to obtain plaintext data. While the United States does not have explicit statutory authorization for law enforcement to conduct hacking operations to gather evidence, law enforcement can engage in lawful hacking pursuant to warrants.[143]

Finally, the BMI created a new agency in 2017, called the Central Office for Information Technology in the Security Sphere (Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)), to focus on telecommunications surveillance, deciphering encrypted communications, and data collection.[144] The German government invested €10 million in the agency in its first year and the agency is expected to increase its workforce from 120 in 2017 to 400 by 2022.[145] ZITiS is expected to play a major role in Germany's lawful hacking and other security efforts moving forward.[146]

---

[141] *Id.*

[142] Bleiker, *supra* note 139.

[143] *See generally* FED. R. CRIM. P. 41; Susan Hennessey, *Lawful Hacking and the Case for a Strategic Approach to "Going Dark"*, BROOKINGS INST. (Oct. 7, 2016), https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/; Susan Hennessey & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, LAWFARE (July 28, 2016), https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques.

[144] Pressemitteilung [Press Release], *Startschuss für ZITiS*, BUNDESMINISTERIUM DES INNERN (Jan. 20, 2017), https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/01/zitis-vorstellung.html.

[145] *Id.*

[146] Ben Knight, *Hacking for the Government: Germany Opens ZITiS Cyber Surveillance Agency*, DEUTSCHE WELLE (Sept. 14, 2017),

Thus, Germany has chosen not to pursue any type of lawful access mandate, and has instead decided to embrace unbreakable encryption and engage in lawful hacking to gain access to plaintext data for law enforcement and intelligence purposes. A significant amount of the debate over encryption technologies and lawful hacking has focused mainly on individual privacy and the German Constitution's robust protections of fundamental rights. The wariness of government surveillance capabilities stems from the country's experience with oppressive fascist and socialist regimes that engaged in massive surveillance.[147]

German technology companies (who will likely remain unconstrained by any type of lawful access mandate) could potentially take advantage of a reputational hit that U.S. technology companies could suffer among foreign consumers if the U.S. enacts a lawful access mandate for encryption of messages in transit. A 2016 study of worldwide encryption products found that Germany had the second highest number of entities that sold or freely offered encryption products (behind only the United States) with 112 products.[148] Germany's Digital Agenda 2014–2017 called for the nation to become the world's leading country in encryption technologies, and Germany may achieve this goal if U.S. encrypted communications applications became less popular as a result of a lawful access mandate for encryption of messages in transit if consumers viewed U.S. products as conduits for U.S. law enforcement or intelligence agencies, or as less secure because they would not offer unbreakable encryption. However, consumers seem to mostly care about being able to be connected to friends, having easy to use and reliable products, and having sleek interfaces and useful applications, and seem willing to sacrifice some privacy and security in exchange so there may be reason to doubt that a significant percentage of consumers would readily move away from U.S. products after a lawful access mandate for encryption of messages in transit to German products as long as U.S. products

http://www.dw.com/en/hacking-for-the-government-germany-opens-zitis-cyber-surveillance-agency/a-40511027.

[147] Konstantin Von Notz, *The Challenge of Limiting Intelligence Agencies' Mass Surveillance Regimes*, *in* PRIVACY AND POWER: A TRANSATLANTIC DIALOGUE IN THE SHADOW OF THE NSA-AFFAIR 331, 338–39 (Russell A. Miller ed. 2017).

[148] SCHNEIER, SEIDEL & VIJAYAKUMAR, *supra* note 31, at 4.

continued to lead in the areas consumers care about the most.[149] Nonetheless, a large number of consumers may move away from U.S. products and U.S.-based companies that produce encrypted communications products may relocate to Germany as a result of a U.S. lawful access mandate for encryption of messages in transit. These companies may fear losing any market share, even if it is not a substantial percentage because of most consumers' greater concern with other factors besides privacy and security, or may have ideological reasons for insisting on the ability to continue to offer unbreakable end-to-end encryption.[150] Many of the developers of these products are small businesses that have a greater ability to

---

[149] *See* ALEXANDER DE LUCA ET AL., EXPERT AND NON-EXPERT ATTITUDES TOWARDS (SECURE) INSTANT MESSAGING 147–51 (2016) (finding that privacy and security only played a minor role in people's decisions to use a particular mobile instant messenger for people in the U.S., the UK, and Germany, and that the primary reason that most participants in the study gave for using a mobile instant messenger was whether their friends used the messenger).

[150] *See* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 118 (2018) (characterizing many technologists as subscribing to the "Californian Ideology," which is a "worldview that is simultaneously countercultural in lifestyle, laissez-faire in economics, and libertarian in politics"); PETER SWIRE, THE DECLINING HALF-LIFE OF SECRETS: AND THE FUTURE OF SIGNALS AND INTELLIGENCE 6 (2015), https://na-production.s3.amazonaws.com/documents/2.26Declining_Half_Life_of_Secrets.pdf (describing an anti-secrecy and libertarian culture among technologists); Andy Greenberg, *Meet Moxi Marlinspike, The Anarchist Brining Encryption to All of Us*, WIRED (July 31, 2016), https://www.wired.com/2016/07/meet-moxie-marlinspike-anarchist-bringing-encryption-us/ (discussing Moxie Marlinspike's, a security researcher who developed Signal and helped encrypt WhatsApp, advocacy of encryption, and Marlinspike's belief that people should be able to use encryption to break the law because this may inspire social change in some areas); Metz, *supra* note 13 (observing that it is "an article of faith that's commonly held among Silicon Valley engineers" that "online privacy must be protected against surveillance of all kinds" and that "[i]n Silicon Valley, strong encryption isn't really up for debate. Among tech's most powerful leaders, it's orthodoxy"); Amy Zegart, *Policymakers are From Mars, Tech Company Engineers are From Venus*, LAWFARE (June 6, 2016), https://www.lawfareblog.com/policymakers-are-mars-tech-company-engineers-are-venus (describing the "the yawning cultural divide between policymakers in Washington and engineers in Silicon Valley tech companies" as the "suit-hoodie divide"); Amy Zegart, Senior Fellow, Hoover Inst., Co-Dir., Stanford Ctr. for Int'l Sec. & Cooperation, Weapons of Mass Deception: The Changing Cyber Landscape (Mar. 27, 2018), https://www.strausscenter.org/event/518-a-conversation-with-amy-zegart.html (same).

relocate their businesses than large technology companies, who often have invested heavily in infrastructure in the United States and have many more reasons to stay in the United States.[151]

Germany does not seem to have large technology companies that could displace U.S. companies or significantly reduce U.S. companies' market share if the U.S. enacted a lawful access mandate for device encryption, but Apple could potentially suffer reduced sales in Germany because of such a mandate. Germany's own technology market is largely dominated by foreign companies. Google's Android operating system has about 69% market share of the mobile operating system market and Apple's iOS has about 30% market share of the mobile operating system market in Germany as of February 2019.[152] Windows' operating system has about 77% market share of the desktop operating system market and Apple's macOS has about 14% market share of the desktop operating system market in Germany as of February 2019.[153] Apple faces stiff competition in the mobile vendor market in Germany, though, and as of February 2019 has about 30% market share, which is below Samsung's nearly 43% market share, but still above Huawei's about 14% market share in Germany.[154] Apple could potentially suffer reduced mobile device sales in the German market if the U.S.

---

[151] *See, e.g.*, Barry Jaruzelski, *Why Silicon Valley's Success is so Hard to Replicate*, SCI. AM. (Mar. 14, 2014), https://www.scientificamerican.com/article/why-silicon-valleys-success-is-so-hard-to-replicate/ (discussing factors that have made Silicon Valley successful and why others have not been able to emulate Silicon Valley's success); Steven Levy, *Apple's New Campus: An Exclusive Look Inside the Mothership*, WIRED (May 16, 2017), https://www.wired.com/2017/05/apple-park-new-silicon-valley-campus/ (reporting that Apple spent $5 billion to build its new headquarters); Matt Tait, *Decrypting the Going Dark Debate*, LAWFARE (Oct. 17, 2017), https://www.lawfareblog.com/decrypting-going-dark-debate (acknowledging that many developers of end-to-end encryption applications are small businesses).

[152] *Mobile Operating System Market Share Germany*, STAT COUNTER, http://gs.statcounter.com/os-market-share/mobile/germany (last visited Mar. 28, 2019).

[153] *Desktop Operating System Market Share Germany*, STAT COUNTER, http://gs.statcounter.com/os-market-share/desktop/germany (last visited Mar. 28, 2019).

[154] *Mobile Vendor Market Share Germany*, STAT COUNTER, http://gs.statcounter.com/vendor-market-share/mobile/germany (last visited Mar. 28, 2019).

enacted a lawful access requirement for device encryption because German consumers are more likely than other consumers to focus on the security and privacy of particular products and services, and German consumers may view Apple's compliance with a lawful access mandate for device encryption in the U.S. as a sign that U.S. law enforcement or intelligence agencies could gain access to their information—even if a lawful access mandate for device encryption would require physical access to a device and not facilitate remote access in reality.[155] Further, Germany is largely dependent on foreign cloud providers.[156] U.S.-based technology companies dominate the social media market in Germany as Facebook possesses about 56% of the market share, YouTube possesses about 4% of the market share, Twitter possesses about 4% of the market share, and Instagram possesses about 1% of the market share in Germany as of February 2019.[157] Also, Google Chrome has about 47% of the browser market share, Apple's Safari has about 19% of the browser market share, Mozilla's Firefox has about 14% of the browser market share, and Google has about 95% of the search engine market share in Germany as of February 2019.[158]

Thus, U.S. technology products and services seem to dominate many parts of the German technology market. However, Apple could potentially face reduced market share in the mobile vendor market in Germany as a result of a U.S. lawful access requirement for device encryption. Further, German encrypted

---

[155] *See* DE LUCA ET AL., *supra* note 149, at 147–51 (finding that a higher percentage of the participants in the study from Germany stated that the main reason they used a mobile instant messenger was because of privacy and security compared with participants from the U.S. and UK); Steven Levy, *Cracking the Crypto War*, WIRED (Apr. 15, 2018), https://www.wired.com/story/crypto-war-clear-encryption/ (noting that Ray Ozzie's technological proposal to facilitate access to an encrypted device would require authorities to physically have the device in their possession to gain access, and could not be used to facilitate remote access to information on the device).

[156] Herpig & Huemann, *supra* note 113.

[157] *Social Media Stats Germany*, STAT COUNTER, http://gs.statcounter.com/social-media-stats/all/germany (last visited Mar. 28, 2019).

[158] *Browser Market Share Germany*, STAT COUNTER, http://gs.statcounter.com/browser-market-share/all/germany (last visited Mar. 28, 2019); *Search Engine Market Share Germany*, STAT COUNTER, http://gs.statcounter.com/search-engine-market-share/all/germany (last visited Mar. 28, 2019).

communications products may increase in popularity at the expense of U.S. encrypted communications products, and businesses that develop encrypted communications applications may relocate to Germany if the U.S. enacts a lawful access requirement for encryption of messages in transit.

C. UNITED KINGDOM

The United Kingdom has had a robust debate over encryption since at least the early 2000s. The UK passed legislation to aid law enforcement in obtaining plaintext data through compelled decryption in 2000 with the Regulation of Investigatory Powers Act (RIPA). The encryption debate once again heated up in the UK during debates over the Investigatory Powers Act, which was enacted in 2016 and reaffirms and possibly expands the government's power to obtain plaintext information through technical assistance provisions and lawful hacking.

The UK enacted RIPA in 2000 to authorize communications interception and the "acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed."[159] Under Section 49 of RIPA, when UK authorities have lawfully collected "protected information" or are "likely to do so," these authorities may issue "notices" that require persons to convert the "protected information" into an intelligible form or disclose the key to the "protected information."[160] The disclosure requirement must be deemed necessary "in the interests of national security," "for the purposes of preventing or detecting crime," or "in the interests of the economic well-being of the United Kingdom."[161] A person with appropriate authority to issue a Section 49 notice must have a reasonable belief that the person being issued the notice possesses the key to the "protected information," the disclosure

[159] Regulation of Investigatory Powers Act 2000, c. 23 (UK).

[160] *Id.* § 49. Protected information is defined as "any electronic data, which, without a key to the data cannot, or cannot readily: be accessed, or be put into an intelligible form." U.K. HOME OFFICE, INVESTIGATION OF PROTECTED ELECTRONIC INFORMATION REVISED CODE OF PRACTICE 8 (2018) [hereinafter U.K. HOME OFFICE, INVESTIGATION OF PROTECTED ELECTRONIC INFORMATION REVISED CODE OF PRACTICE].

[161] Regulation of Investigatory Powers Act 2000, c. 23, § 49(3) (UK).

requirement is necessary on the grounds specified above, the disclosure requirement is proportionate to what authorities endeavor to achieve by obtaining the information in intelligible form or obtaining the key, and it is not reasonably practicable for authorities to obtain the "protected information" in intelligible form without issuing a Section 49 notice.[162] UK authorities must obtain advice from the National Technical Assistance Centre (NTAC), which is the lead agency for matters relating to processing protected information into intelligible form and the disclosure of keys, before issuing a Section 49 notice to ensure that these authorities are appropriately utilized.[163] A person that knowingly fails to comply with the disclosure request of a Section 49 notice may receive a fine as well as two years in prison, or five years in prison in national security or child indecency cases.[164] It is also a crime under RIPA to disclose information that was required to be kept secret under a Section 49 notice and a person that is guilty of this "tipping-off" offense is subject to five years in prison, a fine, or both.[165] Although RIPA was passed in 2000, these encryption provisions did not come into effect until 2007 when the UK's Home Office issued the code of practice for this part of RIPA because encryption technologies were not adopted as quickly as the government originally thought when it passed the statute.[166] In 2014–2015, NTAC granted 88 out of 89 Section 49 notice applications.[167] The government actually served 37 of these Section 49 notices.[168] Of these 37 notices, people complied in 9 of these cases, people failed to comply in 22 of these cases, and the remainder were still being processed at the time of the

[162] *Id.* § 49(2).

[163] U.K. HOME OFFICE, INVESTIGATION OF PROTECTED ELECTRONIC INFORMATION REVISED CODE OF PRACTICE, *supra* note 160, at 7–10.

[164] Regulation of Investigatory Powers Act 2000, c. 23, § 53(5)–(5A) (UK).

[165] *Id.* § 54(4).

[166] U.K. HOME OFFICE, INVESTIGATION OF PROTECTED ELECTRONIC INFORMATION CODE OF PRACTICE (2007); Jeremy Kirk, *Contested UK Encryption Disclosure Law Takes Effect*, WASH. POST (Oct. 1, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/10/01/AR2007100100511.html; *UK Police Can Now Force You to Reveal Decryption Keys*, THE REGISTER (Oct. 3, 2007), https://www.theregister.co.uk/2007/10/03/ripa-decryption_keys_power/.

[167] OFFICE OF SURVEILLANCE COMMISSIONERS, ANNUAL REPORT OF THE CHIEF SURVEILLANCE COMMISSIONER TO THE PRIME MINISTER AND TO THE SCOTTISH MINISTERS FOR 2014–2015, 2015, HC 126, at 15 (UK).

[168] *Id.*

Chief Surveillance Commissioner's annual report.[169] The government decided not to bring charges in 8 cases where a Section 49 notice had not been complied with, and decided not to proceed with prosecution in 9 cases.[170] The government did obtain 3 convictions during this period for failure to comply with Section 49 notices.[171] Privacy and civil liberty advocates criticized these provisions in RIPA as diminishing people's privacy and possibly forcing individuals to incriminate themselves.[172] On the other side of the debate, people have pointed out that "somebody whose device contains evidence which would be liable to convict him for serious criminality if it could be read might prefer to accept a relatively low prison sentence for refusal to hand over the encryption key."[173] Also, authorities may want to gain access to "protected information" for other investigatory purposes beyond the conviction of just the one individual served with a Section 49 notice. The Section 49 notice is most analogous to court orders to enter passwords into locked devices in the U.S., and the punishment for the failure to comply with a Section 49 notice is analogous to contempt charges in the United States, but the United States may provide additional protections in certain circumstances under the Fifth Amendment as discussed earlier.[174]

In 2016, the UK enacted the Investigatory Powers Act to update government surveillance powers. The Act amended RIPA by granting the newly created Investigatory Powers Commissioner, who is a person that has held or currently holds a high judicial office and is appointed by the Prime Minister to this role, oversight over Section 49 notices.[175] The Act also amended RIPA by expanding Section 49 notices to allow the government to issue such notices when authorities have lawfully obtained "protected information"

[169] *Id.*
[170] *Id.*
[171] *Id.*
[172] *UK Police Can Now Force You to Reveal Decryption Keys*, *supra* note 166.
[173] DAVID ANDERSON Q.C., INDEPENDENT REVIEWER OF TERRORISM LEGISLATION, A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW 146 (2015).
[174] *See supra* Part II.A.
[175] Investigatory Powers Act 2016, c. 25, § 227 (UK); *id.* § 229(3)(e).

that is "secondary data from communications," which is essentially metadata.[176]

The Investigatory Powers Act authorizes the Secretary of State to issue technical capability notices on telecommunications operators under Section 253.[177] The Secretary of State may issue a technical capability notice when "the Secretary of State considers that the notice is necessary for securing that the operator has the capability to provide any assistance which the operator may be required to provide in relation to any relevant authorization," "the Secretary of State considers that the conduct required by the notice is proportionate to what is sought to be achieved by that conduct," and "the decision to give the notice has been approved by a Judicial Commissioner."[178] These technical capability notices may impose obligations on a telecommunications operator to "provide facilities or services" and to remove "electronic protection applied by or on behalf of that operator to any communications or data," as well as to comply with "obligations relating to the handling or disclosure of any information."[179] The provisions to remove "electronic protection" are understood to refer to the decryption of encrypted data, but it is unclear whether these provisions impose a lawful access requirement on end-to-end encryption service providers that do not maintain the capability of decrypting users' messages, which would require these providers to redesign their systems.[180] Prior to issuing a technical capability notice, the Secretary of State must take into account "the likely benefits of the notice," "the likely number of users (if known) of any . . . telecommunications service to which the notice relates," "the technical feasibility of complying with the notice," "the likely cost of complying with the notice," and "any other effect of the notice on the person (or description of person) to whom it relates."[181] The Secretary of State must also take into account "whether what is sought to be achieved by the notice could reasonably be achieved by other less intrusive means," "the public

[176] *Id.* § 271(1), sch. 10(46)(2); *id.* § 16(4).
[177] *Id.* § 253(1).
[178] *Id.*
[179] *Id.* § 253(5).
[180] BHAIRAV ACHARYA ET AL., DECIPHERING THE EUROPEAN ENCRYPTION DEBATE: UNITED KINGDOM 5 (2017).
[181] Investigatory Powers Act 2016, c. 25, § 255(3) (UK).

interest in the integrity and security of telecommunication systems and postal services," and "any other aspects of the public interest in the protection of privacy."[182] Further, the Secretary of State must take into account the technical feasibility and cost of complying with a technical capability notice that would impose an obligation to remove "electronic protection" before issuing such a notice.[183] Technical capability notices may be served on persons outside the UK.[184] This provision is most analogous to CALEA's requirement that telecommunications carriers ensure that their equipment, facilities, and services can comply with authorized electronic surveillance and its provision that telecommunications carriers shall only be responsible for decryption when "the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."[185] The provision is also analogous to FISA and Title III's technical assistance provisions, and the All Writs Act in U.S. law.[186] However, Section 253 may go further than these U.S. laws if it is interpreted to impose a lawful access requirement on end-to-end encryption service providers that do not maintain the capability of decrypting user's messages—which would require these providers to redesign their systems.

Numerous privacy and civil liberties groups and technology companies—including Apple, Facebook, Google, Microsoft, Twitter, Yahoo, and Mozilla—expressed concern about the provision authorizing UK authorities to require telecommunications operators to remove "electronic protection."[187] The Liberal Democrats, who opposed the bill, and privacy, civil liberties, and technology groups argued that the provision would weaken

[182] *Id.* § 2(2); U.K. HOME OFFICE, INTERCEPTION OF COMMUNICATIONS: CODE OF PRACTICE § 8.13 (2018) [hereinafter U.K. HOME OFFICE, INTERCEPTION OF COMMUNICATIONS: CODE OF PRACTICE].
[183] Investigatory Powers Act 2016, c. 25, § 255(4) (UK).
[184] *Id.* § 253(8).
[185] 47 U.S.C. §§ 1002(a), 1002(b)(3) (2012).
[186] 18 U.S.C. § 2518(4) (2012); 28 U.S.C. § 1651 (2012); 50 U.S.C. § 1805(c)(2)(B) (2012).
[187] JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL, DRAFT INVESTIGATORY POWERS BILL: REPORT, 2016, HL 93, HC 651, at ¶ 251-255 (UK) [hereinafter JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL, DRAFT INVESTIGATORY POWERS BILL: REPORT].

encryption and lead to reduced security and privacy for users.[188] Apple stated that it understood the government's intention with the provision was to require the company to remove end-to-end encryption if that was necessary to fulfill a warrant and considered proportional.[189] Some have speculated that the technical capability notices could be used to prevent service providers from deploying end-to-end encryption on future systems they are developing.[190] Witnesses during the legislative process also suggested that the provision would have a negative economic effect.[191] Some warned that the provision could make businesses' data less secure if encryption had to be weakened.[192] Witnesses also stated that the provision would negatively impact UK technology companies and discourage technology companies from being located inside the UK or offering services in the UK because of the perceived requirement to reduce the security of products and services.[193] Further, witnesses worried about the possible implications for services offering end-to-end encryption and other encryption services in which companies

[188] *Id.*; CHRISTOPHER GRAHAM, INFO. COMM'R'S OFFICE, JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL—INFORMATION COMMISSIONERS SUBMISSION ¶ 37 (2015); Samuel Barratt, *Investigatory Powers Bill Shows the Home Office Don't Understand or Care About Privacy*, LIBERAL DEMOCRATS (Mar. 2, 2016), https://www.libdems.org.uk/investigatory-powers-bill.

[189] JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL, DRAFT INVESTIGATORY POWERS BILL: REPORT, *supra* note 187, at 78.

[190] Natasha Lomas, *UK Surveillance Bill Includes Powers to Limit End-to-End Encryption*, TECH CRUNCH (July 15, 2016), https://techcrunch.com/2016/07/15/uk-surveillance-bill-includes-powers-to-limit-end-to-end-encryption/.

[191] JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL, DRAFT INVESTIGATORY POWERS BILL: REPORT, *supra* note 187, at ¶ 260; JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL, WRITTEN EVIDENCE 153, 256 (2016) [hereinafter JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL, WRITTEN EVIDENCE].

[192] JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL, DRAFT INVESTIGATORY POWERS BILL: REPORT, *supra* note 187, at ¶ 260; JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL, WRITTEN EVIDENCE, *supra* note 191, at 153, 256.

[193] JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL, DRAFT INVESTIGATORY POWERS BILL: REPORT, *supra* note 187, at ¶ 260; JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL, WRITTEN EVIDENCE, *supra* note 191, at 153, 256.

do not maintain the ability to access user's communications.[194] Supporters of the Investigatory Powers Act and the provision on requiring operators to remove "electronic protection" stressed that law enforcement and intelligence agencies' ability to acquire communications in an intelligible form would be severely degraded without the provision.[195] During the legislative debates, Lord Earl Howe of the Conservative Party, who is the Deputy Leader of the House of Lords, advocated for the bill by explaining "[e]ncryption is now almost ubiquitous and is the default setting for most IT products and online services. If we do not provide for access to encrypted communications when it is necessary and proportionate to do so then we must simply accept that there can be areas online beyond the reach of the law."[196] Ultimately, Howe and the government found this proposition to be unacceptable, and sought to require companies to "maintain the ability when presented with an authorisation under UK law to access those communications."[197]

The Investigatory Powers Act also included a broad provision on national security notices that could potentially be used to require decryption. A national security notice may require a telecommunications operator "to carry out any conduct, including the provision of services or facilities, for the purposes of . . . facilitating anything done by an intelligence service under any enactment other than [the Investigatory Powers Act]" or "dealing with an emergency," or "to provide services or facilities for the purposes of assisting an intelligence service to carry out its functions more securely or more effectively."[198] The Secretary of State may give a telecommunications operator in the UK a national security notice if "the Secretary of State considers that the notice is necessary in the interest of national security," "the Secretary of State considers

---

[194] JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL, DRAFT INVESTIGATORY POWERS BILL: REPORT, *supra* note 187, at ¶ 260; JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL, WRITTEN EVIDENCE, *supra* note 191, at 153, 256.
[195] Lomas, *supra* note 190.
[196] *Id.*
[197] Alexander J. Martin, *UK Gov Says New Home Sec Will Have Powers to Ban End-to-End Encryption*, THE REGISTER (July 14, 2016), https://www.theregister.co.uk/2016/07/14/gov_says_new_home_sec_iwilli_have_powers_to_ban_endtoend_encryption/.
[198] Investigatory Powers Act 2016, c. 25, § 252(3) (UK).

that the conduct required by the notice is proportionate to what is sought to be achieve by that conduct," and "the decision to give the notice has been approved by a Judicial Commissioner."[199] As with technical capability notices, prior to issuing a national security notice, the Secretary of State must take into account "the likely benefits of the notice," "the likely number of users (if known) of any . . . telecommunications service to which the notice relates," "the technical feasibility of complying with the notice," "the likely cost of complying with the notice," and "any other effect of the notice on the person (or description of person) to whom it relates."[200] The Secretary of State must also take into account "whether what is sought to be achieved by the notice could reasonably be achieved by other less intrusive means," "the public interest in the integrity and security of telecommunication systems and postal services," and "any other aspects of the public interest in the protection of privacy."[201] The Act does contain a limiting provision for this power by prohibiting the Secretary of State from giving a telecommunications operator a national security notice when the "main purpose" of the notice is to require the telecommunications operator to do something for which a warrant or authorization would otherwise be required.[202] This national security notice authority may provide UK authorities with the power to order the decryption of encrypted communications in certain national security investigations and exigent circumstances. The broad language in this provision goes well beyond the authorities provided to U.S. intelligence agencies under FISA.[203]

Further, the Investigatory Powers Act empowers the UK to engage in lawful hacking. Part 5 of the Investigatory Powers Act empowers the government to issue targeted equipment interference warrants to authorize or require "the person to whom it is addressed to secure interference with any equipment for the purposes of obtaining" "communications," "equipment data," or "any other

---

[199] *Id.* § 252(1).
[200] *Id.* § 255(3).
[201] *Id.* § 2(2); U.K. HOME OFFICE, INTERCEPTION OF COMMUNICATIONS: CODE OF PRACTICE, *supra* note 182, § 4.12.
[202] Investigatory Powers Act 2016, c. 25, § 252(5)-(6) (UK).
[203] *See generally* Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1885 (2012).

information."[204] The statute defines equipment as "equipment producing electromagnetic, acoustic or other emission or any device capable of being used in connection with such equipment."[205] The Secretary of State may issue targeted equipment interference warrants based on applications from intelligence services if the warrant is necessary "in the interests of national security," "for the purposes of preventing or detecting serious crime," or "in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security" and necessary "for the purposes of obtaining information relating to the acts or intentions of persons outside the British Islands."[206] Scottish Ministers may issue targeted equipment interference warrants if the warrant is necessary to prevent or detect serious crime and the warrant only authorizes interference with equipment in Scotland or believed to be in Scotland, and the warrant only relates to a person in Scotland or believed to be in Scotland.[207] Law enforcement officials may issue targeted equipment interference warrants if the warrant is necessary to prevent or detect serious crime, and certain law enforcement officials may issue a targeted equipment interference warrant if the official "considers that the warrant is necessary for the purposes of preventing death or any injury or damage to a person's physical or mental health or of mitigating any injury or damage to a person's physical or mental health."[208] In all of these circumstances, the official that issues the targeted equipment interference warrant must determine that the conduct authorized is "proportionate to what is sought to be achieved by that conduct," determine that satisfactory procedures are in place regarding retention and disclosure of the information obtained, and gain approval from a Judicial Commissioner for the issuance of the warrant except in urgent circumstances.[209] Telecommunications operators that are served with a targeted equipment interference warrant must take all steps to give effect to the warrant.[210] Thus, the targeted equipment interference warrant

[204] Investigatory Powers Act 2016, c. 25, § 99 (UK).
[205] *Id.* § 135.
[206] *Id.* § 102.
[207] *Id.* § 103.
[208] *Id.* § 106.
[209] *Id.* §§ 102(1), 102(3), 103(1)-(2), 106(1), 106(3).
[210] *Id.* § 128.

provisions enable UK authorities to engage in lawful hacking operations to obtain plaintext communications, and authorize UK authorities to obtain telecommunications operators' help in engaging in these operations possibly through installing software on consumers' devices that "will copy and forward all communications that are sent or received through that device" to government authorities.[211] These tools were seen as extremely useful to law enforcement because it can facilitate the collection of information that could otherwise not be obtained in intelligible form because of the use of encryption.[212] Although the U.S. does not have explicit statutory authorization for law enforcement to conduct hacking operations to gather evidence, law enforcement can engage in lawful hacking pursuant to warrants and could possibly attempt to compel a company to push software to a device to facilitate surveillance through FISA or Title III's technical assistance provisions or the All Writs Act.[213]

In addition, the Investigatory Powers Act authorizes the Secretary of State to issue bulk equipment interference warrants based on an application of an intelligence service to "obtain overseas-related communications, overseas-related information or overseas-related equipment data."[214] Overseas-related communications, information, or equipment data involve communications that are sent or received by individuals who are outside of the British Islands or information about individuals who are outside of the British Islands.[215] The Secretary of State must determine that the warrant is necessary "in the interests of national

---

[211] *See* Herb Lin, *A Biometric Approach as a partial Step Forward in the Encryption Debate*, LAWFARE (Dec. 3, 2015), https://www.lawfareblog.com/biometric-approach-partial-step-forward-encryption-debate (pointing out that companies already push software updates to consumers and this variation of exploiting vulnerabilities would allow government authorities to create a vulnerability it could exploit on a specific device through this mechanism).

[212] JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL, WRITTEN EVIDENCE, *supra* note 191, at 813.

[213] *See generally* FED. R. CRIM. P. 41; 18 U.S.C. § 2518(4) (2012); 28 U.S.C. § 1651 (2012); 50 U.S.C. § 1805(c)(2)(B) (2012); Manpearl, *supra* note 33, at 83–88.

[214] Investigatory Powers Act 2016, c. 25, § 178 (UK).

[215] *Id.* § 176.

security," "for the purposes of preventing or detecting serious crime," or "in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security" and necessary "for the purposes of obtaining information relating to the acts or intentions of persons outside the British Islands."[216] The Secretary of State must also determine that the conduct authorized is "proportionate to what is sought to be achieved by that conduct," determine that satisfactory procedures are in place regarding the retention and disclosure of the information obtained, and gain approval from a Judicial Commissioner for the issuance of the warrant except in urgent circumstances.[217] The bulk equipment interference warrants are important foreign intelligence gathering tools that authorize the UK to engage in bulk hacking operations for such purposes, which can aid in the collection of information in intelligible form that would otherwise be encrypted. In the U.S., Executive Order 12333 authorizes the NSA to collect signals intelligence (SIGINT) abroad on non-U.S. persons, which can include hacking operations to obtain foreign intelligence information.[218]

The UK has significant authorities to compel companies and people to provide plaintext communications and decrypted data. Also, the UK has lawful hacking powers that can be used to obtain plaintext information that could otherwise not be obtained in intelligible form because of the use of encryption. The UK's legislative regime regarding encryption indicates that UK companies are unlikely to take away market share from U.S.-based technology companies if the U.S. were to enact a lawful access requirement for either device encryption or encryption of messages in transit. UK companies would not be in a position to capitalize on any reputational harm among foreign consumers suffered by U.S. companies as a result of a U.S. lawful access requirement for either device encryption or encryption of messages in transit because UK companies are already subject to substantial lawful access requirements. Further, the UK does not seem to even have a strong

[216] *Id.* § 178.
[217] *Id.*
[218] Exec. Order No. 12,333, 3 C.F.R. p. 200 (1981), *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4085 (2003); Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (2004); Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (2008).

technology industry of its own that could take away market share from U.S.-based technology companies. U.S. technology companies seem to dominate the UK market. Microsoft's Windows has about 36% market share, Apple's iOS has about 28% market share, and Google's Android has about 20% market share of the UK operating system market across all platforms as of February 2019.[219] U.S.-based technology companies also dominate the social media market in the UK as Facebook possesses about 63% of the market share, Twitter possesses about 12% of the market share, and YouTube possesses about 2% of the market share as of February 2019.[220] Further, Google Chrome has about 48% of the browser market share in the UK, Apple's Safari has about 32% of the browser market share in the UK, and Google has about 93% of the search engine market share in the UK as of February 2019.[221] In addition, Apple possesses the highest market share for mobile vendors in the UK with 52% market share as of February 2019.[222]

Thus, the UK does not seem to have technology companies that could replace U.S. companies' market share across the world if the U.S. enacted a lawful access requirement for either device encryption or encryption of messages in transit. The UK's legislative regime regarding encryption technologies means that UK companies would not be in a position to capitalize on any reputational harm suffered by U.S. companies as a result of a U.S. lawful access requirement for either device encryption or encryption of messages in transit because UK companies are already subject to substantial lawful access requirements. Finally, U.S. technology

---

[219] *Operating System Market Share United Kingdom*, STAT COUNTER, http://gs.statcounter.com/os-market-share/all/united-kingdom (last visited Mar. 28, 2019).

[220] *Social Media Stats United Kingdom*, STAT COUNTER, http://gs.statcounter.com/social-media-stats/all/united-kingdom (last visited Mar. 28, 2019).

[221] *Browser Market Share United Kingdom*, STAT COUNTER, http://gs.statcounter.com/browser-market-share/all/united-kingdom (last visited Mar. 28, 2019); *Search Engine Market Share United Kingdom*, STAT COUNTER, http://gs.statcounter.com/search-engine-market-share/all/united-kingdom (last visited Mar. 28, 2019).

[222] *Mobile Vendor Market Share United Kingdom*, STAT COUNTER, http://gs.statcounter.com/vendor-market-share/mobile/united-kingdom (last visited Mar. 28, 2019).

companies are unlikely to lose their substantial market share in the UK market if the U.S. enacted a lawful access requirement for either device encryption or encryption of messages in transit because any company that operates in the UK is already subject to the UK's laws, and is therefore already subject to the UK's technical assistance and equipment interference authorities.

D. CHINA

China has a long history of regulating encryption to improve the competitiveness of Chinese technology firms and promote domestic security. In the last several years, China has enacted security-focused legislation that requires technology companies to provide technical assistance to security services to allow security services to obtain decrypted information. China also has a draft Encryption Law that was released for public comment in April 2017 that seeks to create a more uniform approach to encryption regulation.

China passed a new Counterterrorism Law of the People's Republic of China in December 2015, which went into effect in January 2016.[223] The draft version of the law, which was released in 2014, originally contained a provision that required telecommunications service providers and Internet service providers (ISPs) to install "technical interfaces" in the design of their networks and required service providers that used encryption to file their encryption keys with the Chinese government.[224] The draft law also authorized Chinese public security and national security agencies to require service providers or users to provide technical assistance to decrypt information.[225] Further, the draft law required

[223] Zhonghua Renmin Gongheguo Fan Kongbu Zhuyi Fa (中华人民共和国反恐怖主义法) [Counterterrorism Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 27, 2015, effective Jan. 1, 2016) (China) [hereinafter Counterterrorism Law of the People's Republic of China].

[224] Zhonghua Renmin Gongheguo Fan Kongbu Zhuyi Fa (Cao'an) [Counterterrorism Law of the People's Republic of China (Draft)], art. 15–16 (China).

[225] *Id.* art.16.

telecommunications service providers and ISPs to keep all relevant equipment and data inside China.[226] The provisions mandating telecommunications service providers and ISPs to install "technical interfaces," provide authorities with their encryption keys, and store all relevant data inside China received significant pushback from the international community. In a March 2015 interview, President Barack Obama criticized China's draft law, stating that it "would essentially force all foreign companies, including U.S. companies, to turn over to the Chinese government mechanisms where they could snoop and keep track of all the users of those services . . . so we've made very clear to them that this is something they're going to have to change if they expect to do business with the United States."[227] Ultimately, China removed these especially controversial provisions from the final law, but did still include a broad technical assistance provision. The final version of the law states that "[t]elecomunications operators and internet service providers shall provide technical interfaces, decryption and other technical support assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities in accordance with law."[228] This requirement may be interpreted to authorize security agencies to require companies to provide their encryption keys to Chinese authorities.[229] Failure to comply with this technical assistance provision will result in a fine on the telecommunications operators or ISPs of between 200,000 to 500,000 yuan (which is between about $32,000 to about $80,000), and a fine on the personnel directly responsible for the failure to comply of up to 100,000 yuan (which is about $16,000).[230] These

[226] *Id.* art. 94; Zunyou Zhou, *China's Comprehensive Counter-Terrorism Law*, THE DIPLOMAT (Jan. 23, 2016), https://thediplomat.com/2016/01/chinas-comprehensive-counter-terrorism-law/.

[227] *Exclusive: Full Text of Reuters Interview with President Obama*, REUTERS (Mar. 2, 2015), https://www.reuters.com/article/us-usa-obama-transcript/exclusive-full-text-of-reuters-interview-with-obama-idUSKBN0LY2J820150302.

[228] Counterterrorism Law of the People's Republic of China, *supra* note 223, art. 18.

[229] ADAM SEGAL, CHINA, ENCRYPTION POLICY, AND INTERNATIONAL INFLUENCE 5 (2016).

[230] Counterterrorism Law of the People's Republic of China, *supra* note 223, art. 84 (China).

penalties are increased if the circumstances are deemed "serious."[231] The fine for failing to comply is increased to a fine of 500,000 or more yuan (which is about $80,000 or more) on the telecommunications operators or ISPs and between 100,000 to 500,000 yuan (which is between about $16,000 to about $80,000) on the personnel directly responsible for the non-compliance if the circumstances are "serious."[232] The law also authorizes the public security organs to detain the personnel directly responsible for the failure to comply for between five and fifteen days when the circumstances are "serious."[233] This provision is somewhat similar to CALEA, FISA and Title III's technical assistance provisions, and the All Writs Act in U.S. law on its face, but has more severe enforcement provisions than these U.S. laws, does not include judicial involvement unlike these U.S. laws, and may be interpreted more broadly than these U.S. laws.[234]

China's new Cybersecurity Law of the People's Republic of China came into effect in June 2017.[235] This broad and often vaguely worded law established a legal framework on various cyber issues. The law requires that "[n]etwork operators shall provide technical support and assistance for public security agencies and state security agencies in their efforts to maintain national security and investigate criminal activities."[236] Network operators are defined broadly as "owners, managers and network service providers" of "a system consisting of computers or other information terminals and related equipment that collects, stores, transmits, exchanges, and process

---

[231] *Id.*
[232] *Id.*
[233] *Id.*
[234] 18 U.S.C. § 2518(4) (2012); 28 U.S.C. § 1651 (2012); 47 U.S.C. § 1002(b)(3) (2012); 50 U.S.C. § 1805(c)(2)(B) (2012).
[235] Zhonghua Renmin Gongheguo Wangluo Anquan Fa [Cybersecurity Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017) (China); Chris Mirasola, *Understanding China's Cybersecurity Law*, LAWFARE (Nov. 8, 2016), https://www.lawfareblog.com/understanding-chinas-cybersecurity-law; Samm Sacks, *China's Cybersecurity Law Takes Effect: What to Expect*, LAWFARE (June 1, 2017), https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.
[236] Zhonghua Renmin Gongheguo Wangluo Anquan Fa [Cybersecurity Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), art. 28 (China).

information."[237] This law may enable Chinese authorities to require companies to provide plaintext information upon request. Failure to comply with this technical assistance provision will result in a fine on the network operator of between 50,000 to 500,000 yuan (which is between about $8,000 to about $80,000), and a fine on the personnel directly responsible for the failure to comply of between 10,000 to 100,000 yuan (which is between about $1,600 to about $16,000).[238] Also, the law requires that the "personal information and important data gathered or produced by critical information infrastructure operators during operations within" China must be stored in China.[239] The technical assistance provision in this law is also somewhat similar to CALEA, FISA and Title III's technical assistance provisions, and the All Writs Act in U.S. law on its face, but once again has more severe enforcement provisions than these U.S. laws, does not include judicial involvement unlike these U.S. laws, and may be interpreted more broadly than these U.S. laws.[240]

Further, China released a draft Encryption Law for public comment in 2017.[241] This law will create a systematic framework for encryption if it is enacted, and is viewed as a high-priority for the State Council.[242] Article 20 of the draft Encryption Law states: "People's procuratorates, public security bodies and state security bodies may require telecommunications operators and Internet service providers to provide technological decryption support when necessary for national security or the prosecution of criminal cases. Telecommunication[s] operators and Internet service providers shall cooperate, and maintain the secrecy of relevant circumstances."[243]

---

[237] *Id.* art. 76.
[238] *Id.* art. 69.
[239] *Id.* art. 37.
[240] 18 U.S.C. § 2518(4) (2012); 28 U.S.C. § 1651 (2012); 47 U.S.C. § 1002(b)(3) (2012); 50 U.S.C. § 1805(c)(2)(B) (2012).
[241] COVINGTON & BURLING LLP, CHINA RELEASES DRAFT ENCRYPTION LAW FOR PUBLIC COMMENT 1 (2017), https://www.cov.com/en/news-and-insights/insights/2017/05/china-releases-draft-encryption-law-for-public-comment.
[242] HOGAN LOVELLS, DECRYPTING CHINA'S FIRST CRACK AT A CRYPTOGRAPHY LAW 1 (2017), https://f.datasrvr.com/fr1/517/94470/Decrypting_Chinas_first_crack_at_a_Cryptography_Law.pdf.
[243] Zhonghua Renmin Gongheguo Jiami Fa (Cao'an) [Encryption Law of the People's Republic of China (Draft)], art. 20 (China).

If telecommunications operators or ISPs do not comply with the requirement to provide technological decryption support or provide the requested information to Chinese authorities, the company and the personnel directly responsible for the failure to comply will be fined and the personnel directly responsible for the failure to comply can be detained for five to fifteen days.[244] The amount of the fine is unspecified in the draft law.[245] Also, the draft law contains a provision that prohibits people and organizations from using encryption to engage in activities that the government views as "endangering national security or the social public interest."[246] It is unclear how the government would interpret this broad provision and what the punishment for such activity would be under this draft law. In addition, the draft law has far-reaching enforcement provisions that authorize authorities to conduct on-the-spot investigations, access business information, and seize products, equipment, and facilities to ensure compliance.[247] This law would go well beyond any U.S. law if it goes into effect.

China's severe Internet restrictions extend to encryption products and services. China has blocked access to many encrypted messaging applications. These moves seem to be aimed at squashing political dissent and perceived threats to domestic security.[248] China does have popular domestic encrypted messaging applications, such as WeChat and QQ, which have 980 million and 843 million monthly active users, respectively, as of January 2018, but these services do not offer end-to-end encryption.[249] WeChat and QQ are encrypted in transit and may store communications in plaintext and

[244] *Id.* art. 37.
[245] *Id.*
[246] *Id.* art. 21, 38.
[247] *Id.* art. 27–30.
[248] SEGAL, *supra* note 229, at 5–6.
[249] JAMES A. LEWIS ET AL., THE EFFECT OF ENCRYPTION ON LAWFUL ACCESS TO COMMUNICATIONS AND DATA 6–8 (2017); SEGAL, *supra* note 229, at 6; *Most Popular Global Mobile Messenger Apps as of April 2018, Based on Number of Monthly Active Users (in Millions)*, STATISTA, https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (last visited Apr. 15, 2018).

likely allow the government to obtain plaintext communications when the government demands such information.[250]

Thus, China has significant legislative authorities that empower law enforcement and state security agencies to demand that companies provide decryption support in terrorism investigations and technical support in national security and criminal cases, which may be broadly interpreted to require companies to provide access to plaintext information. China's draft Encryption Law would also impose a broad obligation on companies to provide technical decryption support when Chinese authorities demand if this law goes into effect.[251] U.S. technology companies that operate in China are unlikely to lose market share in the Chinese market as a result of the U.S. enacting a lawful access requirement for either device encryption or encryption of messages in transit because any company that operates in China is already subject to China's laws, and is therefore already legally subject to China's stringent demands. Indeed, the Chinese market has proven too large and important for several U.S.-based technology companies to abandon despite of its harsh laws, regulations, and policies. Businesses and governments in China are expected to spend $234 billion on technology goods and services in 2018, China has about 772 million Internet users as of December 2017, and China is expected to have about 699 million smartphone users in 2018.[252] China accounted for about 20% of Apple's revenue in the first quarter of 2018—China accounted for $17.956 billion out of Apple's $88.293 billion in total revenue—and the Chinese market

[250] AMNESTY INT'L, FOR YOUR EYES ONLY?: RANKING 11 TECHNOLOGY COMPANIES ON ENCRYPTION AND HUMAN RIGHTS 43–45 (2016); Shannon Liao, *How WeChat Came to Rule China*, THE VERGE (Feb. 1, 2018), https://www.theverge.com/2018/2/1/16721230/wechat-china-app-mini-programs-messaging-electronic-id-system.

[251] Zhonghua Renmin Gongheguo Jiami Fa (Cao'an) [Encryption Law of the People's Republic of China (Draft)], art. 20 (China).

[252] Charlie Dai, *China's Tech Market Will Grow by 8% in 2018 and 9% in 2019*, FORRESTER (Jan. 21, 2018), https://go.forrester.com/blogs/chinas-tech-market-will-grow-by-8-in-2018-and-9-in-2019/; *Number of Internet Users in China From December 2006 to December 2017 (in Millions)*, STATISTA, https://www.statista.com/statistics/265140/number-of-internet-users-in-china/ (last visited Apr. 15, 2017); *Number of Smartphones in China from 2013 to 2022 (in Millions)*, STATISTA, https://www.statista.com/statistics/467160/forecast-of-smartphone-users-in-china/ (last visited Apr. 15, 2017).

has been increasingly important for Apple as sales in the U.S., Europe, and Japan have been more stagnate over the last few years.[253] In 2018, Apple began hosting Chinese users' iCloud accounts in a Chinese data center and agreed to store the keys for these Chinese iCloud accounts in China, which means that Chinese authorities will be able to obtain access to this information whenever Chinese legal process, which often does not require independent judicial review as in the U.S., demands.[254]

In the fourth quarter of 2017, Apple had the fifth highest market share in the smartphone market in China with 9.3% market share.[255] Chinese companies held the top four spots in the Chinese smartphone market in the fourth quarter of 2017 as Huawei had 20.4% market share, Oppo had 18.1% market share, Vivo had 15.4% market share, and Xiamo had 12.4% market share.[256] As of February 2019, Google's Android operating system had about 72% market share of the mobile operating system market in China and Apple's iOS had about 26% market share of the mobile operating system market in China.[257] Google Chrome has about 50% of the browser market share in China and Apple's Safari has about 13% of the browser market share in China, while UC Browser (which is owned by the Chinese company Alibaba Group) has about 12% of the browser market share in China and QQ Browser (which is owned by the Chinese company Tencent) has about 10% of the browser

---

[253] *Apple Reports First Quarter Results*, Business Wire (Feb. 1, 2018), https://www.businesswire.com/news/home/20180201006492/en/Apple-Reports-Quarter-Results; David Pierson, *While it Defies U.S. Government, Apple Abides by China's Orders—and Reaps Big Rewards*, L.A. TIMES (Feb. 26, 2016), http://www.latimes.com/business/technology/la-fi-apple-china-20160226-story.html.

[254] Stephen Nellis & Cate Cadell, *Apple Moves to Store iCloud Keys in China, Raising Human Rights Fears*, REUTERS (Feb. 23, 2018), https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060.

[255] Jonathan Chadwick, *China's Smartphone Markets Slips 4.9 Percent in 2017: IDC*, ZDNET (Feb. 6, 2018), https://www.zdnet.com/article/chinas-smartphone-market-declined-15-7-percent-for-q4-2017-idc/.

[256] *Id.*

[257] *Mobile Operating System Market Share China*, STAT COUNTER, http://gs.statcounter.com/os-market-share/mobile/china (last visited Mar. 28, 2019).

market share in China across all platforms as of February 2019.[258] Unlike in many other countries, Google does not dominate the search engine market in China since the company pulled its search engine and many other products from the country in 2010 because of Chinese censorship and cyberattacks that targeted Google, and Baidu (a Chinese company) dominates the market with about 75% market share as of February 2019.[259]

China has a significant technology industry that can increasingly compete with U.S.-based technology companies in the global market.[260] For example, Huawaei has become the biggest challenger to Apple and Samsung in the global smartphone market.[261] However, Chinese companies would not be able to take advantage of any reputational harm among foreign consumers suffered by U.S. companies as a result of a U.S. lawful access requirement for either device encryption or encryption of messages in transit because Chinese companies are already subject to robust and very broad lawful access requirements under Chinese law. Further, U.S. companies could always differentiate themselves from their Chinese counterparts because the U.S. has robust privacy protections engrained in law, independent judicial review, and significant oversight over law enforcement and intelligence agencies, whereas China has overly broad and repressive laws and policies.

---

[258] *Browser Market Share China*, STAT COUNTER, http://gs.statcounter.com/browser-market-share/all/china (last visited Mar. 28, 2019).

[259] Kaveh Waddell, *Why Google Quit China—and Why It's Heading Back*, THE ATLANTIC (Jan. 19, 2016), https://www.theatlantic.com/technology/archive/2016/01/why-google-quit-china-and-why-its-heading-back/424482/; *Search Engine Market Share China*, STAT COUNTER, http://gs.statcounter.com/search-engine-market-share/all/china#monthly-201710-201804 (last visited Mar. 28, 2019).

[260] SEGAL, *supra* note 229, at 8; Paul Mozur, *The World's Biggest Tech Companies Are no Longer Just American*, N.Y. TIMES (Aug. 17, 2017), https://www.nytimes.com/2017/08/17/business/dealbook/alibaba-sales-revenue-first-quarter-profit.html.

[261] Arjun Kharpal, *China's Huawei Could Overtake Apple This Year in Smartphones, Top Analyst Says*, CNBC (Oct. 16, 2017), https://www.cnbc.com/2017/10/16/huawei-could-overtake-apple-this-year-in-smartphones-top-analyst-says.html.

E. RUSSIA

Russia heavily regulates encryption technologies and has a legal regime that enables authorities to obtain plaintext information. A person or company must obtain a license from the Federal Security Service (FSB) in order to develop encryption for information and telecommunications systems, disseminate encryption, or provide encryption services, and "commercial importers of encryption hardware and software into Russia must apply for FSB authorization to import."[262] The FSB can require institutions to provide assistance in carrying out the FSB's assigned responsibilities and the FSB can require telecommunications providers to modify hardware or software, or create other necessary condition, to carry out FSB operations.[263] These authorities can allow the FSB to restrict the encryption technologies that are present within Russia and force companies to assist the organization in its operations, which may include requiring companies to provide plaintext information or modify hardware or software to facilitate the FSB's ability to acquire such information.[264] The U.S. does not have an analogous regulatory regime governing encryption technologies and does not permit law enforcement or intelligence agencies such wide-latitude to require companies to assist these agencies in their operations.[265] The U.S. has much more constrained authorizations that solely require telecommunications carriers to ensure that their equipment, facilities, and services can comply with

---

[262] TAIA GLOBAL INC., RUSSIAN LAWS AND REGULATIONS: IMPLICATIONS FOR KASPERSKY LABS (2012), https://www.wired.com/images_blogs/dangerroom/2012/07/Russian-Laws-and-Regulations-and-Implications-for-Kaspersky-Labs.pdf; Alexander Baj, *OFAC Issues General License Authorizing Certain Dealings with FSB Related to Encryption Import Licensing*, STEPTOE INT'L BLOG (Feb. 2, 2017), https://www.steptoeinternationalcomplianceblog.com/2017/02/ofac-issues-general-license-authorizing-certain-dealings-with-fsb-related-to-encryption-import-licensing/.

[263] TAIA GLOBAL INC., *supra* note 262, at 2.

[264] James Andrew Lewis, *Reference Note on Russian Communications Surveillance*, CTR. FOR STRATEGIC INT'L STUD. (Apr. 18, 2014), https://www.csis.org/analysis/reference-note-russian-communications-surveillance.

[265] *See* DANIEL CASTRO & ALAN MCQUINN, UNLOCKING ENCRYPTION: INFORMATION SECURITY AND THE RULE OF LAW 8 (2016) (describing the U.S.'s shift away from strictly regulating encryption through export controls).

authorized electronic surveillance under CALEA, and enable law enforcement and intelligence agencies to compel companies to provide information primarily under FISA, under the Stored Communications Act (SCA), under Title III, and using pen register and trap and trace devices.[266]

In 2016, Russia enacted new counterterrorism legislation, Federal Law No. 374 on Amending the Federal Law on Counterterrorism and Select Legislative Acts of the Russian Federation Concerning the Creation of Additional Measures Aimed at Countering Terrorism and Protecting Public Safety, that contained multiple provisions expanding the authorities of intelligence and law enforcement agencies.[267] The new law includes requirements for telecommunications providers and ISPs to store the content and metadata of communications for specific periods of time within Russia.[268] The law requires telecommunications providers to store "metadata about all connections, transmissions, and receipts of voice information, written texts, images, sounds, video, and other messages transferred through communications networks" inside Russia for three years.[269] ISPs must store this metadata inside Russia for one year.[270] The contents of communications, messages, and "voice information" from telephone communications must be stored

[266] 18 U.S.C. § 2518(4) (2012); 18 U.S.C. § 2703 (2012); 18 U.S.C. § 3123 (2012); 47 U.S.C. §§ 1002(a), 1002(b)(3) (2012); 50 U.S.C. § 1805(c)(2)(B) (2012).

[267] Federal'nyi Zakon o vnesenii izmeneniy v Federal'nyy zakon "O protivodeystvii terrorizmu" i otdel'nye zakonodatel'nye akty Rossiyskoy Federatsii v chasti ustanovleniya dopolnitel'nykh mer protivodeystviya terrorizmu i obespecheniya obshchestvennoy bezopasnosti [Federal Law on Amending the Federal Law on Counterterrorism and Select Legislative Acts of the Russian Federation Concerning the Creation of Additional Measures Aimed at Countering Terrorism and Protecting Public Safety] 2016, No. 374, *available at* http://publication.pravo.gov.ru/Document/View/0001201607070016.

[268] NIGEL CORY, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION, CROSS-BORDER DATA FLOWS: WHERE ARE THE BARRIERS, AND WHAT DO THEY COST? 28 (2017); Ksenia Koroleva, Latham & Watkins LLP, *"Yarovaya" Law – New Data Retention Obligations for Telecom Providers and Arrangers in Russia*, GLOBAL PRIVACY & SECURITY COMPLIANCE LAW BLOG (July 29, 2016), https://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/.

[269] Peter Roudik, *Russia: New Surveillance Rules*, LIBR. OF CONGRESS (July 18, 2016), http://www.loc.gov/law/foreign-news/article/russia-new-electronic-surveillance-rules/.

[270] *Id.*

inside Russia for six months.[271] Technology companies stated that these storage requirements would require massive financial investments that exceeded the annual revenue of some companies.[272] Reports indicated that companies would need to spend RUB 2.2 trillion, which is about $35.5 billion, to comply with this law.[273] However, these financial concerns did not deter Russian legislators from passing the bill. The U.S. does not have analogous data retention laws.[274]

The 2016 law also requires telecommunications providers and ISPs to forward the metadata or content to Russian security services upon request, without a court order.[275] Further, the law imposes fines on Internet providers for the use of encryption that was not previously certified or licensed of up to RUB 40,000, which is about $650.[276] The law requires information-distribution organizations to provide the FSB with all information and keys required to decode electronic communications information.[277] Refusal to provide this information will result in a fine of up to a RUB 1 million fine, which is about $16,000.[278] This is quite different from the U.S. approach, which typically requires prior judicial approval to acquire information under FISA, under Title III, under the SCA, and using pen register and trap and trace devices.[279] The U.S. can issue administrative subpoenas, grand jury subpoenas, and national security letters to obtain certain information without prior judicial approval, but subpoenas and national security letters

---

[271] *Id.*

[272] Matthew Bodner, *What Russia's New Draconian Data Laws Mean for Users*, THE MOSCOW TIMES (July 13, 2016), https://themoscowtimes.com/articles/what-russias-new-draconian-data-laws-mean-for-users-54552.

[273] *Id.*

[274] However, the Federal Communications Commission (FCC) does require that carriers retain "the name, address, and telephone number of the caller, telephone number called, date, time and length of the call" for 18 months. 47 C.F.R. § 42.6 (2018).

[275] Roudik, *supra* note 269.

[276] *Id.*

[277] *Id.*

[278] *Id.*; *Irina Yarovaya's 'Anti-Terrorist' War on Civil Rights*, MEDUZA (June 22, 2016), https://meduza.io/en/feature/2016/06/22/irina-yarovaya-s-anti-terrorist-war-on-civil-rights.

[279] 18 U.S.C. § 2518 (2012); 18 U.S.C. § 2703 (2012); 18 U.S.C. § 3123 (2012); 50 U.S.C. § 1804 (2012).

are subject to judicial review if a recipient makes a motion to modify or quash the subpoena or when judicial enforcement action occurs, and are much more narrowly tailored than the broad requirement in this 2016 Russian law.[280] Further, the U.S. does not have a requirement that companies must provide the government with all information and keys required to decode electronic communications information.

Shortly after this law was passed, Privacy Internet Access, a virtual private network (VPN) provider, announced that it was leaving Russia because Russian authorities seized some of the company's servers inside the country.[281] The company believed that its servers were seized as a way to enforce the new law because the company does not store data as is required under the statute.[282] Global technology companies, especially major U.S.-based companies, appear to not be complying with the statute's requirement to disclose encryption keys to the FSB and other requirements.[283] In April 2018, Russia blocked Telegram, an encrypted messaging service that offers end-to-end encryption, from operating in the country because Telegram refused to comply with the statute's requirement to provide the FSB with encryption keys to enable the FSB to obtain plaintext communications.[284]

---

[280] *See generally* DOYLE, ADMINISTRATIVE SUBPOENAS AND NATIONAL SECURITY LETTERS IN CRIMINAL AND INTELLIGENCE INVESTIGATIONS: A SKETCH, *supra* note 46; DOYLE, ADMINISTRATIVE SUBPOENAS IN CRIMINAL INVESTIGATIONS: A BRIEF LEGAL ANALYSIS, *supra* note 46; DOYLE, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: LEGAL BACKGROUND, *supra* note 46; U.S. DEP'T OF JUSTICE, OFFICE OF LEGAL POLICY, *supra* note 46.

[281] *We are Removing our Russian Presence*, PRIV. INTERNET ACCESS (July 2016), https://www.privateinternetaccess.com/forum/discussion/21779/we-are-removing-our-russian-presence.

[282] *Id.*

[283] Scott J. Shackelford, *iGovernance: The Future of Multi-Stakeholder Internet Governance in the Wake of the Apple Encryption Saga*, 42 N.C. J. Int'l L. 883, 914–15 (2017); Shaun Waterman, *Tech Giants Silent on new Russian Surveillance Law*, FED SCOOP (July 22, 2016), https://www.fedscoop.com/russia-vpn-yarovaya-law-encryption-2016/.

[284] Neil MacFarquhar, *Russian Court Bans Telegram App After 18-Minute Hearing*, N.Y. TIMES (Apr. 13, 2018), https://www.nytimes.com/2018/04/13/world/europe/russia-telegram-

Thus, Russia heavily regulates encryption technologies and has robust lawful access requirements that do not even require judicial review or have independent oversight. As Russia's security services have become more powerful and unchecked in recent years, objections to the government's approach to encryption technologies has done little to persuade decision makers. U.S. technology companies are unlikely to lose market share in the Russian market if the U.S. enacts a lawful access requirement for either device encryption or encryption of messages in transit because any company that operates in Russia is already subject to Russia's laws—although Russia does not appear to have strictly enforced all of its requirements against major U.S. technology companies—and are therefore already legally subject to Russia's stringent demands.

American technology companies have a significant presence in the Russian market. As of June 2018, Google's Android operating system had about 74% market share of the mobile operating system market in Russia and Apple's iOS had about 24% market share of the mobile operating system market in Russia.[285] As of February 2019, Google Chrome has about 58% of the browser market share in Russia, Apple's Safari has about 9% of the browser market share in Russia, Mozilla's Firefox has about 6% of the browser market share in Russia, and Google has about 46% of the search engine market share in Russia.[286] Apple has the highest market share in the mobile vendor market in Russia as of February 2019 with about 29% market share, too.[287] In addition, U.S.-based social media companies have significant penetration in the Russian market. In the fourth quarter of 2017, YouTube had 63% market penetration, WhatsApp

encryption.html; *Russia Seeks to Block Telegram Messaging App*, BBC (Apr. 6, 2018), http://www.bbc.com/news/technology-43668537.

[285] *Market Share Held by Mobile Operating Systems in Russia From January 2012 to June 2018*, STATISTA, https://www.statista.com/statistics/262174/market-share-held-by-mobile-operating-systems-in-russia/ (last visited Mar. 28, 2019).

[286] *Browser Market Share Russian Federation*, STAT COUNTER, http://gs.statcounter.com/browser-market-share/all/russian-federation (last visited Mar. 28, 2019); *Search Engine Market Share Russian Federation*, STAT COUNTER, http://gs.statcounter.com/search-engine-market-share/all/russian-federation (last visited Mar. 28, 2019).

[287] *Mobile Vendor Market Share Russian Federation*, STAT COUNTER, http://gs.statcounter.com/vendor-market-share/mobile/russian-federation (last visited Mar. 28, 2019).

had 38% market penetration, Facebook had 35% market penetration, Instagram had 31% market penetration, Google+ had 30% market penetration, and Facebook Messenger had 11% market penetration.[288]

Russia does not appear to have significant global technology companies that could take away market share worldwide from U.S.-based technology companies if the U.S. enacts a lawful access requirement for either device encryption or encryption of messages in transit.[289] Finally, Russian companies would not be able to take advantage of any reputational harm among foreign consumers suffered by U.S. companies as a result of a U.S. lawful access requirement for either device encryption or encryption of messages in transit even if Russian companies were able to compete globally because Russian companies are already subject to strict lawful access requirements under Russian law. Russia's stringent laws also make it extremely unlikely that any companies that produce encrypted communications applications would relocate to Russia as a result of a U.S. lawful access mandate for encryption of messages in transit.

[288] *Penetration of Leading Social Networks in Russia as of 4th Quarter 2017*, STATISTA, https://www.statista.com/statistics/284447/russia-social-network-penetration/ (last visited Mar. 28, 2019).

[289] *See* ANDREY MOVCHAN, DECLINE, NOT COLLAPSE: THE BLEAK PROSPECTS FOR RUSSIA'S ECONOMY 5–10, 13–17, 19–21 (2017), http://carnegie.ru/2017/02/02/decline-not-collapse-bleak-prospects-for-russia-s-economy-pub-67865 (describing Russia's reliance on oil and gas and lack of technology products and services as well as lack of investment in the technology industry); Dmitriy Frolovsky, *Russia's Innovation Façade*, THE DIPLOMAT (Feb. 7, 2017), https://thediplomat.com/2017/02/russias-innovation-facade/ (criticizing Russia's lack of innovation); *see also* Andrew Higgins, *Russia Wants Innovation, But it's Arresting its Innovators*, N.Y. TIMES (Aug. 9, 2017), https://www.nytimes.com/2017/08/09/world/europe/vladimir-putin-russia-siberia.html.

IV. HOW THE INTERNATIONAL FRONT OF THE GOING DARK DEBATE AFFECTS THE U.S. ENCRYPTION DEBATE

The increasing prevalence of encryption and concern among law enforcement and intelligence agencies that they are "going dark" as a result and will no longer be able to obtain information that they have the legal authority to acquire has sparked a rigorous debate and even inspired legislative action in some countries. The debates in France, Germany, and the United Kingdom share numerous similarities with the debate in the United States. As with the United States, concerns about terrorism and solving crime are driving the desire to create lawful access requirements in France and the UK, and in Germany in the case of de Maizière joining France's ministers of interior in calling on the European Commission to enact a lawful access requirement at the EU level. Supporters of a lawful access requirement in France have also espoused nationalistic sentiments and a desire to exert sovereign authority over multinational technology companies based in the U.S. that some lawmakers view as refusing to cooperate with law enforcement and intelligence authorities. The debates in these countries have typically not distinguished between lawful access requirements for device encryption and lawful access requirements for encryption of messages in transit.

Those who oppose any form of lawful access requirement in these countries primarily argue that such a requirement would decrease user security and privacy, and could negatively impact businesses because companies depend on strong cybersecurity in the modern world. Some who oppose any lawful access mandate in these countries also argue that such a requirement could hurt technology companies by creating the perception that these companies' products and services are less secure. In Germany, the government has sought to become the world's leader in encryption technologies, which it sees as an economic opportunity, which has been part of the push away from a lawful access requirement in the country.

Ultimately, the UK has enacted significant authorities to compel companies and people to provide plaintext information and lawful hacking powers that can be used to obtain plaintext information that could otherwise not be obtained in intelligible form because of encryption. France has proposed legislation to mandate a lawful access requirement and several of these proposals came quite close to being enacted in 2016, but ultimately failed to pass. However, President Macron has called for authorities to have access to plaintext information and France may try again to pass a lawful access requirement, especially if France's efforts pushing for more robust action at the EU-level are not successful or the country suffers another terrorist attack. On the other hand, Germany has chosen not to pursue any type of lawful access requirement and has embraced unbreakable encryption and lawful hacking to gain access to plaintext data.

Security concerns have also led China to mandate companies to provide broad technical support that may be interpreted to require companies to provide plaintext information, and may drive China to require companies to provide technical decryption support. Similarly, security concerns have prompted Russia to take robust legislative action to regulate encryption and require lawful access without significant legal process. However, there has not been robust debate regarding encryption in either China or Russia as these authoritarian governments do not have the same open debates about the proper legislative, regulatory, and policy approach to issues as Western democracies.

U.S. technology products and services largely dominate the global market, which is especially true in France, Germany, and the UK. U.S. technology companies also have a very significant presence in China and Russia. These companies' success has been extremely important for the U.S.'s economy. The greatest potential harm from a lawful access requirement for either device encryption or encryption of messages in transit likely stems from the possible decrease in the market share and economic viability of U.S. companies due to foreign consumers switching away from American products and online services to foreign technology companies based on the belief that their communications would be accessible to U.S. law enforcement or intelligence agencies if they

continued to use U.S. products and services. The encryption debates in France, Germany, the UK, China, and Russia indicate that Germany is likely the only country examined in this Article that could potentially take advantage of a lawful access requirement for either device encryption or encryption of messages in transit in the U.S. because Germany has chosen to embrace unbreakable encryption and not to pursue any type of lawful access requirement. While France has not enacted a lawful access requirement yet, the robust debate in the country and possibility that the Macron government will push for such measures make it seem unlikely that U.S. products and services would suffer grave reputational harms among French consumers if the U.S. enacted a lawful access requirement for either device encryption or encryption of messages in transit. The debate in France also makes it unlikely that U.S.-based companies that produce encrypted communications applications would relocate to France as a result of a U.S. lawful access mandate for encryption of messages in transit.

German technology companies could potentially take advantage of a reputational hit that U.S. technology companies could suffer among foreign consumers if the U.S. enacts a lawful access mandate for encryption of messages in transit. Germany already has a high number of encryption products and desires to be the world's leading country in encryption technologies. A U.S. lawful access mandate for encryption of messages in transit may lead consumers to move away from U.S. encrypted communications applications, U.S.-based end-to-end encryption services to relocate to Germany, and to more encrypted communications applications being based in Germany. U.S.-based companies that produce encrypted communications products may relocate to Germany out of fear of losing market share or may have ideological reasons for insisting on the ability to continue to offer unbreakable end-to-end encryption. Further, there are many encrypted communications applications, and "it is easy to change and install apps and many of the developers of these apps are small businesses overseas that the U.S. government can't efficiently regulate."[290] Therefore, a U.S. lawful access mandate for encryption of messages in transit could result in a reduction of the percentage of the world's

[290] Tait, *supra* note 151.

communications that transit the United States as more consumers may adopt foreign products and more applications may be based outside the U.S. This would result in greater difficulty for U.S. intelligence and law enforcement agencies in obtaining information. Although encrypted communications applications may not be able to provide plaintext information upon receipt of lawful process, these companies may still be able to provide metadata, which can be useful information for intelligence and law enforcement agencies. If more of these companies were based in Germany, or in other countries not examined in this Article that may chose not to pursue lawful access mandates for encryption of messages in transit, the U.S. would be less likely to be able to obtain even metadata from these companies during an investigation. While the shift to overseas encrypted communications applications may not be widespread among illicit actors because most illicit actors are not sophisticated, as discussed *supra*, some illicit actors will likely shift to use these services. Further, although these encrypted communications applications are unlikely to develop into major technological companies of the same scale as Facebook, Apple, or Alphabet's Google, these applications are able to generate significant revenue streams through offering special features that users can purchase, having advertisements, or having a subscription based model.[291] For example, in 2017, Forbes estimated that WhatsApp could generate between about $5 billion to over $15 billion in annual revenue in the next few years if Facebook is able to implement an effective strategy to monetize the service based on the annual revenues that WeChat and Line, a communications application, generate.[292] This means that these encrypted communications applications have the potential to be significant economic contributors.

However, Germany does not seem likely to be able to take advantage of a reputational hit that U.S. technology companies

[291] Juro Osawa, *Messaging Apps Make Money*, WALL ST. J. (Mar. 3, 2014), https://blogs.wsj.com/digits/2014/03/03/how-messaging-apps-make-money/; Vanessa Page, *How WhatsApp Makes Money*, INVESTOPEDIA (May 1, 2018), https://www.investopedia.com/articles/personal-finance/040915/how-whatsapp-makes-money.asp; *How Much Revenue Can WhatsApp Generate?*, FORBES (Nov. 10, 2017), https://www.forbes.com/sites/greatspeculations/2017/11/10/how-much-revenue-can-whatsapp-generate/#48d361782f2c.

[292] *How Much Revenue Can WhatsApp Generate?*, *supra* note 291.

could suffer among foreign consumers if the U.S. enacts a lawful access mandate for device encryption. Germany does not seem to have large technology companies that could displace U.S. companies that manufacture operating systems and produce devices, or significantly reduce those U.S. companies' market share. Apple's iOS and Google's Android operating system dominate the global market for mobile operating systems; Microsoft's Windows, Apple's macOS, and Google's Android dominate the operating system market across all platforms; and Apple has a significant share of the global mobile vendor market.[293] These U.S.-based companies would almost certainly not leave the United States in response to a lawful access mandate for device encryption given the significant infrastructure present in the U.S. and established pool of talent among other factors, and Germany is unlikely to be able to develop or attract a company of a similar status that can compete with these U.S.-based giants that already dominate the global market.[294]

China is likely the only nation studied in this Article with a significant technology industry that can increasingly compete with U.S.-based technology companies in its domestic market and in the global market. However, Chinese companies would not be able to take advantage of any reputational harm among foreign consumers suffered by U.S. companies as a result of a U.S. lawful access requirement for either device encryption or encryption of messages in transit because Chinese companies are already subject to robust and very broad lawful access requirements under Chinese law. To the extent consumers make decisions based on security and privacy concerns, U.S. companies could always differentiate themselves from their Chinese counterparts because the U.S. has robust privacy protections engrained in law, independent judicial review, and

---

[293] *Device Vendor Market Share Worldwide*, STAT COUNTER, http://gs.statcounter.com/vendor-market-share/mobile (last visited Apr. 27, 2018); *Mobile Operating System Market Share Worldwide*, STAT COUNTER, http://gs.statcounter.com/os-market-share/mobile/worldwide (last visited Apr. 27, 2018); *Operating System Market Share Worldwide*, STAT COUNTER, http://gs.statcounter.com/os-market-share (last visited Apr. 27, 2018).

[294] *See, e.g.*, Jaruzelski, *supra* note 151 (discussing factors that have made Silicon Valley successful and why others have not been able to emulate Silicon Valley's success); Levy, *supra* note 151 (reporting that Apple spent $5 billion to build its new headquarters).

significant oversight over law enforcement and intelligence agencies, whereas China has overly broad and repressive laws and policies.

Thus, U.S. technology companies appear unlikely to lose market share or economic viability as a result of a lawful access requirement for device encryption, but U.S.-based encrypted communications applications may suffer a significant loss of market share and economic viability as a result of a lawful access requirement for encryption of messages in transit. As long as U.S. companies that produce operating systems and devices continue to lead in being able to connect users to friends, having easy to use and reliable products, and having sleek interfaces and useful applications, while still making the most secure products and services possible that comply with a lawful access requirement for device encryption, U.S. companies will likely continue to dominate these areas of the technology market. U.S. policymakers should be much more cautious in pursuing a lawful access requirement for encryption of messages in transit, though, because U.S.-based encrypted communications applications could suffer a great deal or decide to relocate to another country, such as Germany, as a result of a lawful access requirement for encryption of messages in transit.