A HOOVER INSTITUTION ESSAY

The Encryption Debate in Europe

DANIEL SEVERSON

Aegis Paper Series No. 1702

Introduction

The going dark debate has spread to Europe. During the past few years, Europeans have suffered a wave of terrorist attacks, even as the commercial use of strong encryption technology has increased.[1] In response, Europeans are debating to what extent their governments should require access to encrypted data—either independently or with active cooperation from communications service providers (CSPs).[2] This article examines changes to encryption laws since 2015, with a particular focus on recent statutes and regulations in France, the United Kingdom, the Netherlands, Hungary, and Poland.

Studying the encryption debate in Europe is important for a variety of reasons. To combat terrorism and other transnational crime, the United States must look beyond its borders. A study of what other countries are currently doing can help the United States strike the appropriate balance between privacy and security while writing and implementing its own laws and policies. New legislation in other countries could affect the operation of mutual legal assistance treaties and the availability of evidence gathered from investigations abroad. It could affect the legal obligations of US-based companies that provide services in Europe. The decisions of European countries may influence the legal and policy discussion elsewhere and may even set the standard for applicable legislation in some places (for instance, the United Kingdom for the Commonwealth countries and France for its former colonies). The laws and regulations that European countries pass may also affect the availability of encryption products, as laws change the incentives in their creation, production, and use. Whereas the United States accounts for a plurality of all encryption hardware or software, two-thirds of the world's encryption products originate outside the United States, and European countries (including Germany, the United Kingdom, France, and Sweden) are collectively the next biggest source of encryption products.[3]

Daniel Severson is a Harvard Law School and Harvard Kennedy School graduate. All statements of fact, analysis, or opinion are those of the author and do not reflect the official policy or position of the US Government. Thank you to Jack Goldsmith, Ben Wittes, and the Hoover Working Group on National Security, Technology, and Law for their input and support. Heartfelt thanks to Amy Goldfeder for her questions, insight, and advice.

The discussion proceeds by examining the most recent legislation in France, the United Kingdom, the Netherlands, Hungary, and Poland. The conclusion offers some brief thoughts about the different approaches in Europe as compared to the United States.

France

French statutes already require operators to provide technical assistance in furnishing information during a terrorism or criminal investigation, and a new counterterrorism law significantly enhances the financial penalties for failure to comply.

In October 2016, France adopted the Digital Republic Law, which updated the legal regime for the country's digital economy, including new rules for net neutrality, access to government data, and data privacy.[4] Notably, during the yearlong debate of the bill, the French National Assembly rejected an amendment that might have required mandatory back doors for products using encryption. Following the November 13, 2015, terrorist attacks in Paris, Nathalie Kosciusko-Morizet, a former spokesperson for Nicholas Sarkozy and a senior member of the right-leaning Les Républicains Party, introduced a broadly worded amendment: "Technology manufacturers must take into consideration the necessity of granting to the police, pursuant to an investigation and after judicial authorization, access to hardware. A decree from the State Council sets the rules for the application of this article."[5]

Although hastily drafted, the amendment was designed to launch a debate and called for "France to take the initiative" to "prevent individual encryption systems from impeding investigations."[6] The amendment could have allowed the State Council to require electronics manufacturers to build back doors into their products. Security experts worried the amendment would have discouraged companies operating in France from designing or providing strong encryption at all.[7] However, Minister of Digital Affairs Axelle Lemaire—who called the proposal "vulnerability by design"—succeeded in getting the National Assembly to reject it.[8] Members of Parliament do not appear to have proposed any subsequent encryption-related amendments to the bill, and the statute includes none.

In fact, the statute as enacted actually recognizes the importance of encryption technology for protecting what France calls the "right to private life." A small but potentially important provision modifies the mission of the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés, or CNIL), an independent agency charged with applying data privacy laws. Notably, part of CNIL's mission is to keep abreast of changes in information technology and inform the public of how those changes affect privacy rights.[9] The new provision expressly requires

CNIL to "promote, as part of its mission, the use of technologies that protect privacy, including data encryption technologies."[10] The Digital Republic Law empowers CNIL to impose significantly higher administrative fines for violations of privacy laws and regulations, and including encryption in CNIL's mandate further signals France's commitment to enhancing data privacy.[11]

On the other hand, in the wake of recent terrorist attacks, France has also adopted new legislation that increases law enforcement access to encrypted data. Two weeks after the November 13, 2015, terrorist attacks in Paris, the French Parliament enacted the International Electronic Communications Law, which revised a previous restructuring of France's surveillance powers and authorized the interception of foreign communications.[12] French authorities can collect foreign intelligence to promote the national defense and other fundamental national interests, including not only combating terrorism but also advancing major scientific, economic, and industrial interests.[13] Under the law's data retention limits, French authorities can store foreign communications for up to one year and metadata for up to six years.[14] But if the information is encrypted, then the security services can store such data for up to eight years after collection, and the one-year limit does not start to run until the data is decrypted or exploited.[15] Moreover, in cases of "strict necessity," French authorities can keep encrypted data indefinitely.[16]

A new counterterrorism law has provided another arena for France to debate decryption requirements. Enacted in June 2016 through accelerated procedures, the new law significantly increases financial penalties for refusal to provide technical assistance in decrypting communications as part of a criminal or terrorism investigation. The counterterrorism law amended article 434-15-2 of the French Criminal Code, which has been in force since November 2001, to impose a three-year prison term and a 270,000-euro fine for "anyone who has knowledge of a secret decryption key for an encryption standard that may have been used to prepare, facilitate or commit a crime or offense" and who refuses to provide or use such decryption keys in cooperation with the authorities.[17] If cooperation "would have prevented a crime or limited its effects," the penalties increase to five years in prison and a 450,000-euro fine.[18]

Although these fines are six times higher than the original law,[19] the fines actually represent a compromise in the legislative process. The Senate version of the bill would have increased the fine for refusal to decrypt to only 150,000 euros.[20] But proposed

amendments in the National Assembly would have imposed exceptionally high penalties.

For example, an amendment proposed by Les Républicains deputy Éric Ciotti would have required telecommunications manufacturers and operators, as well as internet service providers, to hand over to the authorities all communications relevant to a terrorism investigtion.[21] Violations would have resulted in a maximum fine of two million euros and a ban of up to one year on marketing products and services in France.[22] In support of the amendment, Deputy Ciotti noted that, according to a special computer science unit of the French judicial police, at least 8 cell phones of the 133 analyzed in 2015 could not be "treated." Those inaccessible phones included an iPhone 4S, seized in connection with the investigation of the November 13 attacks in Paris, and the mobile phone of Sid Ahmed Ghlam, who had planned to attack a church in Villejuif in 2015.[23]

Two other amendments by Socialist deputy Yann Galut would have increased fines to one million euros in circumstances in which electronic equipment designers refuse to cooperate in providing access to data relevant to an ongoing investigation.[24] In support of those measures, Deputy Galut and his colleagues cited a *New York Times* op-ed from August 2015 by the Manhattan district attorney, Cyrus R. Vance Jr., and the Paris chief prosecutor, François Molins, which warned about going dark.[25]

Although it increased fines for refusal to decrypt, the French Parliament dropped other proposals mandating technical assistance, including one that would have targeted heightened penalties at companies like Apple whose products and services are encrypted. For example, in response to the Apple-FBI dispute, the National Assembly initially adopted an amendment to the counterterrorism bill that would have imposed large fines (up to 350,000 euros) and substantial prison terms (up to five years) on corporate executives who refuse to provide data encrypted using encryption technology their companies had developed.[26] In the Senate's Committee of Laws Report, the rapporteur agreed that private firms that create encryption should face high penalties for refusing to help the authorities in investigations but argued that some of the text that emerged from the National Assembly was "superfluous and counterproductive."[27] The committee dropped the specific, heavy penalties—350,000 euros in fines and five years in prison—reasoning that the introduction of those penalties would confuse the organization of the criminal code and, more important, that a different part of the criminal code already penalizes such conduct.[28]

Parliament also dropped another aggressive provision. Article 60–1 of the French Code of Criminal Procedure stipulates that failure to provide promptly to the judicial police information "relevant" or "useful for ascertaining the truth" in a terrorism investigation results in a 3,750-euro fine.[29] The National Assembly's version of the bill would have enhanced that penalty to a 15,000-euro fine and two years of imprisonment. The Senate Committee of Laws cut the prison sentence, noting that prison time would be "disproportionate" and would violate the necessity principle for criminal sentences, especially for a single failure to respond to a government request, rather than a refusal.[30] Those penalties had apparently never been enforced,[31] and the joint parliamentary committee ultimately dropped the provision altogether.

The introduction of these amendments produced an intense debate, with American tech multinationals like Apple and Google front and center. During the National Assembly's first meeting, Deputy Ciotti argued that heavy penalties were required "when faced with companies whose market capitalization reaches several hundred billion dollars, who consider state governments dwarfs, and who show contempt for the law."[32] He therefore proposed a temporary ban on marketing as "the only way to signal to these companies that their financial incentives will never surpass the laws of a democratic state."[33] In the same vein, Deputy Galut emphasized that multinationals have effectively "decided to enact their own legislation" and that frustrating investigations is "unacceptable."[34] The rapporteur for the Committee of Laws, Pascal Popelin, condemned refusals to cooperate by tech giants acting "in the name of a pseudo-defense of liberties" and trying to "justify the unjustifiable."[35] He noted that although the government can already require decryption under other provisions of the French Code, those provisions do not set specific penalties for noncompliance.

On the other hand, another deputy observed that the debate is not a simple one of pitting multinationals completely insensitive to terrorism against judges singularly pursuing the truth in investigations. He also cautioned, "Think about what could happen to decryption keys in the hands of authoritarian regimes, like China, North Korea, or Syria."[36]

Ultimately, Minister of Justice Jean-Jacques Urvoas asked the deputies to withdraw their amendments. "A national law is ineffective," he said. Only "international cooperation" can provide an effective solution.[37] He assured the deputies that the French government was already working with Brussels for a solution at the European Union (EU) and that Robert Gelli, the director of the Department of Criminal Affairs of the Ministry of Justice, was meeting with American officials.[38]

What do we make of these developments? France had strong provisions for requiring technical assistance,[39] and Parliament enhanced financial penalties for refusal to cooperate drastically—by six times. At the same time, France has so far not adopted mandatory back doors. Unsurprisingly, France's data protection authority, CNIL, has endorsed strong encryption and opposed back doors.[40] But so too has the French Network and Information Security Agency (ANSSI),[41] an inter-ministerial agency that is responsible for the government's cyber defense and reports to the prime minister; ANSSI recently drafted a confidential memo supporting robust encryption and objecting to back doors.[42] That these French agencies have recently expressed support for strong encryption standards suggests that any renewed proposals for back-door access would face resistance. As the rash of legislative proposals after the November 13 attacks and the extended state of emergency demonstrate, however, another terrorist attack could prompt renewed efforts to provide aggressive counterterrorism powers. Indeed, earlier, on Bastille Day, President François Hollande explained that the state of emergency must end, but he reversed himself hours later when a man drove a truck through a crowd in Nice, killing at least eighty-four people.[43] Parliament extended the state of emergency for a fourth time. In December 2016 it voted again—for the fifth time—to extend the state of emergency. In force since the November 2015 terrorist attacks, the state of emergency now extends through July 15, 2017, covering the two-round presidential elections in April and May and parliamentary elections in June.[44]

United Kingdom

Since 2007, the United Kingdom has authorized compelled decryption under the Regulation of Investigatory Powers Act. The Investigatory Powers Act of 2016 preserves and expands those powers, mandating technical assistance in decrypting communications pursuant to a warrant, and leaving open the power to require companies to decrypt end-to-end encrypted communications.

In 2000, the United Kingdom enacted the Regulation of Investigatory Powers Act (RIPA), and decryption is a central feature of the statute. The preamble clarifies that the act seeks to provide for not only the "interception of communications" but also "the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed."[45] Part III of the act regulates "Investigation of Electronic Data Protected by Encryption Etc."[46] Notably, when the government comes into lawful possession of "protected information,"[47] certain officials can issue so-called Section 49 Notices requiring persons to disclose an encryption key or put information into intelligible form.[48] The law authorizes Section 49 Notices if they are

"necessary" (1) in the interests of national security, (2) to detect or prevent crime, or (3) in the interests of the economic well-being of the United Kingdom.[49] The secretary of state may provide appropriate compensation to help offset the cost of compliance.[50] But anyone who refuses to comply faces up to two years' imprisonment, or five years in a national security or child indecency case.[51] Section 49 Notices can also include prohibitions on "tipping off"—that is, with the exception of seeking legal advice, anyone served with such notices must keep that fact secret. "Tipping-off" can incur a fine, imprisonment up to five years, or both.[52]

Although the UK Parliament enacted RIPA in 2000, the Home Office decided not to immediately implement the decryption provisions because people did not start using encryption as quickly as anticipated.[53] Decryption powers only came into force on October 1, 2007, when the Home Office issued a code of practice.[54] Unlike France, which has so far reportedly not enforced its decryption laws,[55] the United Kingdom has enforced Section 49 Notices. The annual reports of the Office of the Surveillance Commissioners provide statistics from the National Technical Assistance Centre (NTAC), a unit under Government Communications Headquarters (GCHQ, the United Kingdom's NSA) that handles data recovery, decryption, and analysis.[56] For the period 2014–15, NTAC granted eighty-eight out of eighty-nine applications for Section 49 Notices. Among them, the government served thirty-seven notices, and in at least twenty-two cases people failed to comply. In most of those cases, the government decided not to charge or, alternatively, prosecute for noncompliance. Still, in 2014–15 alone the government secured three convictions for noncompliance with Section 49 Notices.[57] Although the numbers of approvals and notices served have increased since 2007, the number of convictions has ranged from one to three;[58] for instance, NTAC reported three convictions for the 2012–13 period and two convictions for the 2013–14 period.[59]

In 2016 the UK Parliament enacted the Investigatory Powers Act,[60] a detailed and technical 291-page law that updates and consolidates the United Kingdom's surveillance authorities for the intelligence and security services, as well as law enforcement.[61] Dubbed the Snoopers' Charter, the law provides for interception and retention of communications content and metadata, as well as equipment interference (that is, hacking) and decryption. For the first time in the United Kingdom, the law also introduces judicial supervision of warrants authorizing those powers.[62] As relevant here, the new law modifies existing decryption powers and creates new ones.

The Investigatory Powers Act leaves investigations of encrypted data under RIPA Part III—including Section 49 Notices—largely intact, subject to a couple of significant modifications.[63] Notably, the Investigatory Powers Act brings Section 49 Notices under the consolidated oversight powers of a new Investigatory Powers Commissioner (IPC), who must review the government's use of investigatory powers and make annual reports to the prime minister. Not only must the IPC independently keep investigations of electronic information protected by encryption under scrutiny,[64] but law enforcement authorities must also notify the IPC whenever a Section 49 Notice requires a person to disclose an encryption key (rather than simply put the requested information in intelligible form).[65] The new law also expands the scenarios in which Section 49 Notices can be issued: whereas RIPA authorized them whenever the government obtained protected information pursuant to lawful interception of "communications," the Investigatory Powers Act also allows such notices whenever the government obtains protected information by intercepting merely "secondary data from communications"—that is, metadata.[66] Thus, however the government obtains protected information, or—and this is important—"is likely to do so," it can compel disclosure of the information in intelligible form.[67]

Beyond modifying the powers in Part III of RIPA, the Investigatory Powers Act creates new, potentially broader statutory powers to compel decryption. In creating new powers, the act does not use the word encryption, perhaps to remain technology-agnostic or to keep provisions intentionally obscure. Pursuant to section 253, the secretary of state may serve "technical capability notices" on telecommunications operators to facilitate assistance with authorizations under the act.[68] The range of obligations the government can impose through technical capability notices is extensive: the government can require an operator to not only furnish an indefinite range of devices, facilities, or services, but also remove "electronic protection applied by or on behalf of [an] operator to any communications or data," as well as comply with "obligations relating to the handling or disclosure of any information" (what appears to be a catch-all clause).[69] The act charges the secretary of state with implementing those broad powers through applicable regulations; after consulting with a Technical Advisory Board and other interested stakeholders, she has discretion to do so.[70]

The secretary of state may give a technical capability notice if she determines that it is necessary and proportionate and if a judicial commissioner approves.[71] In issuing such notices, the secretary of state must also consider the cost and technical feasibility

of compliance, as well as the likely number of affected users.[72] The government can serve a technical capability notice on persons outside the United Kingdom (and require action outside the United Kingdom).[73] The act does not impose any time limits on technical capability notices—instead, they extend for however long the secretary of state considers a "reasonable" period.[74]

Not surprisingly, these broad provisions have proven controversial. Tech firms including Apple, Facebook, Google, Microsoft, Mozilla, Twitter, and Yahoo raised concerns in written testimony on the draft bill, including the prospect of the government preventing them from providing end-to-end encryption.[75] On February 11, 2016, the UK Parliament's Joint Committee issued its report on the bill with the following recommendations related to encryption:

> We agree with the intention of the Government's policy to seek access to protected communications and data when required by a warrant, while not requiring encryption keys to be compromised or backdoors installed on to systems. The drafting of the Bill should be amended to make this clear. (Recommendation 16)
>
> The Government still needs to make explicit on the face of the Bill that CSPs offering end-to-end encrypted communication or other un-decryptable communication services will not be expected to provide decrypted copies of those communications if it is not practicable to do so. We recommend that a draft Code of Practice should be published alongside the Bill for Parliament to consider. (Recommendation 17)[76]

In its formal response, the UK government claimed that it had addressed the committee recommendations:

> The revised Bill makes clear that obligations to remove encryption from communications only relate to electronic protections that have been applied by, or on behalf of, the company on whom the obligation has been placed and/or where the company is removing encryption for their own business purposes.

The government further claimed that

> [t]he Bill has also been revised to make clear that where an obligation is placed on a CSP which includes the removal of encryption, the technical feasibility, and likely cost of complying with those obligations must be taken into account.[77]

The government's claims only partly address the committee's recommendations. The government also issued a draft Code of Practice for Interception of Communications, which clarifies that the scope of the obligation to remove encryption applies only to companies that have applied encryption themselves.[78] And the final act does require the secretary of state to take into account the technical feasibility and likely cost of a technical capability notice.[79] But technical feasibility and cost considerations were already included in the draft bill dated November 2015.[80] More important, the final act does not provide guidance on how to determine whether an obligation is not technically feasible or too costly. For instance, does the law require a telecommunications operator to invest resources to develop a capability to decrypt? What counts as technically feasible—an individual CSP's capabilities or an industry leader's? When is compliance not technically feasible because it would compromise the overall security of an electronic system?[81]

In a nod to privacy advocates, the final act does require any public authority considering whether to issue a technical capability notice to weigh "the public interest in the integrity and security of telecommunication systems and postal services."[82] But the new law does not unambiguously disclaim the power to require decryption of end-to-end encrypted messages through services like WhatsApp or iMessage. Based on the committee debate in Parliament, some observers even worry that the government could use technical capability notices to *prevent* CSPs from securing *future* systems using end-to-end encryption.[83]

At one point, the government issued a fact sheet on encryption, acknowledging the benefits that flow from encryption (such as protected personal information, intellectual property, and e-commerce) and maintaining that the bill does not require installing back doors.[84] The government, however, removed this fact sheet from its website.[85] A different fact sheet on CSPs asserts that RIPA already requires CSPs to maintain the ability to remove any encryption that they apply and that the bill "does not impose any additional requirements in relation to encryption over and above the existing obligations in RIPA."[86] If that were true, however, it would make little sense for Parliament to add an extended section on technical capability notices. That it did so suggests that those notices provide additional powers. In the main, the new power appears to be *ex ante* statutory authorization for decryption. Whereas under RIPA the government can issue Section 49 Notices once it "come[s] into possession" of protected information or "is likely to do so,"[87] under the Investigatory Powers Act the government can issue technical capability notices to require CSPs to *actively maintain*

infrastructure and capabilities to decrypt promptly and securely.[88] With technical capability notices, the government need not wait until it comes into possession of protected information, and the statute sets no time limit on these notices, so long as they are "reasonable."[89] Thus, neither the statute nor the government's guidance documents unambiguously disclaims construction of back doors or measures that undermine encryption standards, as the committee had recommended.

Finally, it should be noted that the government could use another provision in the Investigatory Powers Act—national security notices—to require decryption or other extraordinary measures. National security notices provide broad powers "requiring the operator to take such specified steps as the Secretary of State considers necessary in the interests of national security," such as "facilitating anything done by an intelligence service under any enactment other than" the act, "dealing with an emergency," or "provid[ing] services or facilities for the purpose of assisting an intelligence service to carry out its functions more securely or more effectively."[90] The UK government has stated that this power replaces the "power of direction" under the Telecommunications Act of 1984 and will be used "very sparingly."[91] An important limitation on national security notices is that the government cannot use them to mandate actions the "main purpose of which is to do something for which a warrant or authorization" would otherwise be required under the act.[92] Therefore, the government cannot use national security notices to avoid getting warrants or authorizations for intercepting communications or technical capability notices. But the "main purpose" language could be flexibly interpreted, and the government could presumably enlist the powers under that provision in extraordinary circumstances—such as during a perceived significant terrorist attack—to require decryption.

The Netherlands

The Netherlands has so far rejected encryption back doors but has existing statutory technical assistance requirements.

Following the Paris attacks of November 2015 and suggestions that the terrorists may have used encryption, the Netherlands' House of Representatives asked the Dutch cabinet to adopt a position on encryption. In a letter dated January 4, 2016, the ministers of security and justice and economic affairs provided a balanced assessment of the trade-offs encryption entails.[93]

In support of strong encryption, the letter notes that encryption protects citizen data handled by the government, secures diplomatic and military communications,

and supports the right to privacy.[94] Notably, the ministers explain the benefits of encryption for the Dutch economy:

> Being able to use encryption strengthens the international competitive position of the Netherlands and contributes to an attractive business and innovation climate for, for example, start-ups, data centres and cloud computing. Confidence in secure communication and data storage is essential for the (future) growth potential of the Dutch economy, which is mainly in the digital economy.[95]

At the same time, the letter emphasizes that encryption "complicates, delays or renders it impossible to (timely) gain insight into . . . communication[s] for the benefit of protecting national security and investigating criminal offences."[96] The letter soberly recognizes that "[t]here are currently no options" for granting technical access to law enforcement without making encryption products simultaneously vulnerable to criminals, terrorists, and foreign intelligence services.[97] The letter concludes:

> The cabinet endorses the importance of strong encryption for internet security to support the protection of personal privacy of citizens, for confidential communication of the government and companies and for the Dutch economy.
>
> The cabinet is therefore of the opinion that at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption in the Netherlands.[98]

The Dutch cabinet thus recommended against legislation mandating encryption back doors or other restrictive measures.

While the media focused on this conclusion,[99] it is important to point out that the Netherlands already has broadly worded statutory provisions authorizing decryption, including technical assistance requirements. The Intelligence and Security Services Act of 2002 authorizes Dutch security services to break into "an automated work" or otherwise conduct surveillance on communications transferred across such "automated works," such as by "introduc[ing] technical devices to undo the encryption of data stored or processed in the automated work."[100] The same statute includes specific technical assistance provisions that require "[a]ny person who has knowledge of the undoing of the encryption of the data stored or processed in the automated work . . . upon the written request of the head of the service to provide all the co-operation

necessary in order to undo the encryption."[101] The Dutch Code of Criminal Procedure similarly provides that for cases involving serious offenses like terrorism the public prosecutor can require a person "reasonably presumed to have knowledge of the manner of encryption of the communications . . . to assist in decrypting the data by either providing this knowledge, or undoing the encryption."[102]

It is also worth noting that the Dutch cabinet letter calls for international cooperation. "The situation in the Netherlands cannot be separated from its international context," the letter says. "Considering the wide availability and application of advanced encryption techniques and the cross-border nature of data transaction, room for national action is limited."[103]

Hungary

Hungary declined to ban end-to-end encryption but issued new regulations on access to encrypted communications in terrorism investigations.

Hungary recently enacted amendments to its E-Commerce Act that affect encryption.[104] Under the new rules, CSPs remain free to choose whether to employ end-to-end encryption. If they do, the law grants the government authority to obtain the metadata of encrypted communications. If CSPs do not use end-to-end encryption, the law enables the government to request a company to monitor and turn over an individual user's full text, audio, and video communications data. The amendments create new regulatory enforcement procedures and introduce fines of HUF 10 million (about $35,000) per offense.[105]

Notably, as originally drafted, the legislation would have banned end-to-end encryption.[106] With the intention of empowering law enforcement to detect and disrupt terrorism, the proposed legislation would have required developers to create back doors,[107] and smart phone users who used end-to-end encryption would have risked up to two years in prison.[108] Opposition parties objected to those proposals and succeeded in removing them from the final legislation.

Poland

Poland also declined to ban encryption but seeks EU-level legislation.

On February 7, 2016, Poland enacted a new surveillance law that grants law enforcement increased access to digital data. The law does not prohibit or regulate encryption.[109] In fact, Poland's Code of Criminal Procedure does not require persons

to provide encryption keys or passwords—instead, it provides that criminal suspects or accused persons are not obliged to provide incriminating evidence.[110]

Poland, however, appears to prefer international action to regulate encryption. In submissions to the Council of the European Union, Poland has called for EU law to "encourage software/hardware manufactures to put some kind [of] 'backdoors' for LEA [law enforcement authorities] or to use only relatively weak cryptographic algorithms."[111] Hungary, Croatia, Latvia, and Italy have also reportedly pushed for legislation at the EU level.[112] Just last summer, the interior ministers of France and Germany—two countries that have recently suffered significant terrorist attacks—called for the European Commission to enact a law that would enable European governments to seek court orders compelling decryption.[113]

Conclusion

The United States Congress has so far declined to provide express statutory authorization for decryption, though members of Congress have floated bills to do so.[114] The American approach instead relies on judges to address government requests for access to or disclosure of encrypted data on a case-by-case basis under broad legal principles. Authorization for this dates back to the 1789 All Writs Act, which broadly empowers US federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[115] Cases involving decryption can also implicate a suspect's Fifth Amendment right to refrain from testimonial self-incrimination.[116] Because neither of these legal rules expressly contemplates compelled decryption or changes concrete incentives, we might call the US legal regime a "wait-and-see" approach.

Europe's approach—statutory authorization to compel decryption—differs from the US approach. Following a spate of terrorist attacks, Europe has debated how to regulate encryption. No European country has gone so far as to ban encryption or mandate preinstalled back doors.[117] Although the United Kingdom's Investigatory Powers Act does not expressly reject such power, and the act's technical capability notices could be construed to authorize them, the head of GCHQ recently declared his opposition to "banning encryption" or "mandatory backdoors."[118] But even as they have disavowed back doors, European countries have sought to preserve and supplement law enforcement tools to detect and disrupt terrorism and serious crime. For France this means severe sanctions for failure to cooperate in decrypting information. For the United Kingdom and the Netherlands it means statutory requirements for technical

assistance in decrypting data. For Hungary and Poland it means introducing new encryption regulations and seeking additional action at the EU level.

The US approach leaves it up to judges to adapt rulings to particular circumstances, with the consequence that, in disputes over government access to encrypted data, the outcome often remains uncertain. Indeed, the standoff between Apple and the FBI over unlocking the iPhone used by a gunman in the San Bernardino attack had reached a stalemate until an Israeli firm offered to help the FBI access the device.[119]

The European approach does not resolve this uncertainty. In fact, even though some European countries have adopted technical assistance provisions, there remains uncertainty in implementation and enforcement, as well as the weighing of statutory factors like cost, technical feasibility, and privacy rights. Still, the European approach establishes some guiding parameters. By criminalizing noncompliance with statutory decryption orders, European countries have changed incentives for CSPs, developers, and individual users. Those measures may increase government access to encrypted data. It is important to note, however, that the measures will not always have their desired effect, particularly in the most extreme cases. Because terrorism and other serious crimes (like sex offenses) carry substantial prison terms upon conviction, persons under investigation for such crimes may decide to refuse to comply with a notice to decrypt and risk only a shorter term of imprisonment.[120]

Ultimately, the fundamental policy question involving encryption is how to balance competing values: promoting privacy, protecting dissidents, and spurring economic growth, while also preventing crime and mitigating its destructive consequences. Answering this question effectively is difficult because, even if we can identify the relevant factors for consideration, we do not yet know the magnitude of the costs and benefits of different legal and policy approaches. But in considering encryption law and policy, Europe will continue to provide an important reference point, one that affects the discussion in the United States and other countries around the world.

NOTES

1 *See* Chertoff Group, The Ground Truth About Encryption 7 (2016) (describing how technology companies have shifted toward making encryption "on" the default setting in hardware and software). I adopt the Chertoff Group's definition of encryption: "the encoding of data or information in a way that is intended to prevent access to that data or information by persons or parties whose access is not authorized by the creator of the data." *Id.* at 1. Encryption, or secret writing, can take various forms. With

endpoint encryption a user holds the encryption key locally on her device. End-to-end encryption involves encryption of messages in transit without using servers. Service providers can also provide encryption, for instance when they encrypt email and cloud storage on their servers. Id. at 4–5.

2 *See, e.g.*, European Parliament, Resolution of 25 November 2015 on the Prevention of Radicalisation and Recruitment of European Citizens by Terrorist Organisations (2015/2063[INI]) (raising "serious concerns over the increasing use of encryption technologies by terrorist organisations that make their communications and their radicalisation propaganda impossible for law enforcement to detect and read, even with a court order").

3 Bruce Schneier et al., "A Worldwide Survey of Encryption Products" (Feb. 11, 2016), https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf.

4 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 Française [J.O.] [Official Gazette of France], Oct. 8, 2016, p. 235, https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=689260AE5CAF2A74BA1806E0C4ADDD67.tpdila17v_1?cidTexte=JORFTEXT000033202746&categorieLien=id.

5 Digital Republic Bill (No. 3318), Amendment No. CL92 (Jan. 4, 2016) (Fr.), http://www.assemblee-nationale.fr/14/amendements/3318/CION_LOIS/CL92.asp.

6 *Id*.

7 *See* Joshua Eaton, *With or Without Evidence, Terrorism Fuels Combustible Encryption Debate,* Christian Sci. Monitor (Mar. 28, 2016), http://www.csmonitor.com/World/Passcode/2016/0328/With-or-without-evidence-terrorism-fuels-combustible-encryption-debate.

8 *See* Guillaume Champeau, *Chiffrement: Le Gouvernment Rejette les Backdoors,* Numerama (Jan. 13, 2016), www.numerama.com/politique/138689-chiffrement-le-gouvernement-rejette-les-backdoors.html; *see also* Liam Tung, *Encryption Backdoors by Law? France Says "Non,"* ZDNet (Jan. 18, 2016, 12:39 PM), http://www.zdnet.com/article/encryption-backdoors-by-law-france-says-non/; Jeff John Roberts, *France Rejects "Backdoors" Law to Defeat Encryption,* Fortune (Jan. 13, 2016, 12:45 PM), http://fortune.com/2016/01/13/france-encryption/.

9 Loi 78-17 du 6 janvier 1978 modifée art. 11(4) (Fr.), https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee#Article1.

10 Loi 2016-1321 du 7 octobre 2016 pour une République numérique art. 59(2)(f) (Fr.), https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=689260AE5CAF2A74BA1806E0C4ADDD67.tpdila17v_1?cidTexte=JORFTEXT000033202746&categorieLien=id.

11 For an overview of the Digital Republic Law, see Olivier Proust & Gaetan Goossens, *France Adopts Digital Republic Law,* Field Fisher (Oct. 4, 2016, 10:59 AM), http://privacylawblog.fieldfisher.com/2016/france-adopts-digital-republic-law/.

12 Loi 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationals [Law 2015-1556 of November 30, 2015 on International Electronic Communications], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Dec. 1, 2015, p. 22,185.

13 Code de la Sécurité Intérieure art. 811-3 (Fr.), https://www.legifrance.gouv.fr/affichCode.do;jsessionid=EB7E1CB999CD31779A3967D448C9619B.tpdila17v_1?idSectionTA=LEGISCTA000030935034&cidTexte=LEGITEXT000025503132&dateTexte=20170129.

14 Code de la Sécurité Intérieure art. 854-5 (Fr.), https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=279B93BCE1C89CA30D48D9BE0715558E.tpdila17v_1?idArticle

=LEGIARTI000031550341&cidTexte=LEGITEXT000025503132&dateTexte=20170129&categorieLien=id&oldAction=&nbResultRech=.

15 *Id.* Encrypted data associated with "subscription numbers or identifiers" traceable to the French "national territory" enjoy a slightly shorter data retention limit of six years, but the time delay and "strict necessity" exceptions still apply. *See* Code de la Sécurité Intérieure art. 822-2 (Fr.), https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=279B93BCE1C89CA30D48D9BE0715558E.tpdila17v_1?idArticle=LEGIARTI000030935068&cidTexte=LEGITEXT000025503132&dateTexte=20170129&categorieLien=id&oldAction=; Code de la Sécurité Intérieure art. 854-8 (Fr.), https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000025503132&idArticle=LEGIARTI000031550357&dateTexte=&categorieLien=cid.

16 *Id.*

17 Code Pénal art. 434-15-2 (Fr.), https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=CD80FBE41F7648FD56B1C5D53B5AC1F3.tpdila23v_1?idArticle=LEGIARTI000032654251&cidTexte=LEGITEXT000006070719&categorieLien=id&dateTexte=.

18 *Id.*

19 Previously the fines were 45,000 euros and 75,000 euros, respectively.

20 Bill to Combat Organized Crime, Terrorism, and Their Financing art. 4 *quinquies* (Senate version of Mar. 23, 2016), http://www.senat.fr/leg/pjl15-492.html.

21 Bill to Combat Organized Crime, Terrorism, and Their Financing (No. 3515), Amendment No. 221 (Feb. 25, 2016), http://www.assemblee-nationale.fr/14/amendements/3515/AN/221.asp.

22 *Id.*

23 *Id.*

24 Bill to Combat Organized Crime, Terrorism, and Their Financing (No. 3515), Amendment No. 532 (Feb. 29, 2016), http://www.assemblee-nationale.fr/14/amendements/3515/AN/532.asp; Bill to Combat Organized Crime, Terrorism, and Their Financing (No. 3515), Amendment No. 533 (Feb. 29, 2016), http://www.assemblee-nationale.fr/14/amendements/3515/AN/533.asp.

25 Cyrus R. Vance Jr. et al., *When Phone Encryption Blocks Justice,* N.Y. Times (Aug. 11, 2015), http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?_r=1.

26 Bill to Combat Organized Crime, Terrorism, and Their Financing (No. 3515), Amendment No. 90 (Feb. 23, 2016), http://www.assemblee-nationale.fr/14/amendements/3515/AN/90.asp.

27 Bill to Combat Organized Crime, Terrorism, and Their Financing (No. 3515), Commission of Laws Report (No. 491) (Mar. 23, 2016), http://www.senat.fr/rap/l15-491-1/l15-491-17.html.

28 *See id.* France's National Consultative Commission on the Rights of Man opposed these enhanced penalties because it thought current statutory provisions were already sufficient, the contemplated provisions were not "necessary and proportional," and the proposed provisions would violate the right to private and family life enshrined in Article 8 of the European Convention on Human Rights. *See* National Consultative Commission on the Rights of Man, Opinion on the Bill to Combat Organized Crime, Terrorism, and Their Financing (No. 3515) (Mar. 17, 2016), https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032628821&dateTexte=&categorieLien=id.

29 Code de Procédure Pénal art. 60-1 (Fr.), https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071154&idArticle=LEGIARTI000006575048&dateTexte=&categorieLien=cid.

30 *See* Commission of Laws Report, *supra* note 27.

31 Guillaume Champeau, *5 ans de prison en cas de refus de communiquer des données chiffrés,* Numerama (Mar. 3, 2016), http://www.numerama.com/politique/149981-5-ans-de-prison-en-cas-de-refus-de-communiquer-des-donnees-chiffrees.html.

32 Bill to Combat Organized Crime, Terrorism, and Their Financing (No. 3515), National Assembly's First Meeting (Mar. 3, 2016), http://www.assemblee-nationale.fr/14/cri/2015-2016/20160140.asp.

33 *Id.*

34 *Id.*

35 *Id.*

36 *Id.*

37 *Id.*

38 *See id.*

39 The relevant provisions are articles 60-1 and 230-1 of the Code of Criminal Procedure, article 434-15-2 of the Criminal Code, and article 871-1 of the Internal Security Code.

40 *See Les Enjeux de 2016 (3): Quelle Position de la CNIL en Matière de Chiffrement?*, CNIL (Apr. 8, 2016), https://www.cnil.fr/fr/les-enjeux-de-2016-3-quelle-position-de-la-cnil-en-matiere-de-chiffrement.

41 For more information about this agency, see ANSSI, http://www.ssi.gouv.fr/ (last visited July 8, 2016).

42 Martin Untersinger, *La CNIL Très Favorable au Chiffrement des Données*, Le Monde (Apr. 9, 2016, 10:23 AM), http://www.lemonde.fr/pixels/article/2016/04/09/la-cnil-tres-favorable-au-chiffrement-des-donnees_4899172_4408996.html#hWGj18UR5tA1CCWt.99.

43 *See* Alissa J. Rubin et al., *France Says Truck Attacker Was Tunisia Native with Record of Petty Crime*, N.Y. Times (July 15, 2016), http://www.nytimes.com/2016/07/16/world/europe/attack-nice-bastille-day.html?_r=0.

44 Loi 2016-1767 du 19 décembre 2016 prorogeant l'application de la loi 55-385 du 3 avril 1955 relative a l'etat d'urgence, Legifrance, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033651975&categorieLien=id.

45 Regulation of Investigatory Powers Act 2000, c. 23, introductory text (U.K.), http://www.legislation.gov.uk/ukpga/2000/23/introduction.

46 Regulation of Investigatory Powers Act 2000, c. 23, §§ 49–56 (U.K.), http://www.legislation.gov.uk/ukpga/2000/23/part/III.

47 "Protected information" means any electronic data that, without the key to the data, cannot readily be accessed or put into intelligible form. Id. §§ 49, 56(1).

48 *Id.* §§ 49, 50(3)(c).

49 *Id.* § 49(3).

50 *Id.* § 52.

51 *Id.* § 53(5)–(6).

52 *Id.* § 54.

53 *See* Jeremy Kirk, *Contested UK Encryption Disclosure Law Takes Effect,* Wash. Post (Oct. 1, 2007, 10:19 AM), http://www.washingtonpost.com/wp-dyn/content/article/2007/10/01/AR2007100100511.html; Out-Law.com, *UK Police Can Now Force You to Reveal Decryption Keys,* The Register (Oct. 3, 2007, 4:43 AM), http://www.theregister.co.uk/2007/10/03/ripa-decryption_keys_power/.

54 *See* The Regulation of Investigatory Powers (Acquisition and Disclosure of Communications Data: Code of Practice) Order 2007, http://www.legislation.gov.uk/uksi/2007/2197/contents/made; U.K. Home Office, Investigation of Protected Electronic Information: Code of Practice (2007), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97959/code-practice-electronic-info.pdf.

55 Champeau, *supra* note 31.

56 *See The National Technical Assistance Centre,* GCHQ (Aug. 5, 2016), https://www.gchq.gov.uk/features/national-technical-assistance-centre.

57 Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2014–2015 15–16, ¶¶ 4.17–4.22 (2015), http://www.statewatch.org/news/2015/jul/uk-surveillance-comm-annual-report.pdf. The most recent report does not provide data on convictions, but the rate at which NTAC granted Section 49 Notice approvals remained the same, with 87 out of 88 applications granted. Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2015–2016 17, ¶ 4.16 (2016), https://assets.documentcloud.org/documents/3000981/OSC-Annual-Report-2015-2016.txt.

58 For an unofficial summary of the statistics, see *Regulation of Investigatory Powers Act 2000/Part III,* Open Rights Group Wiki, https://wiki.openrightsgroup.org/wiki/Regulation_of_Investigatory_Powers_Act_2000/Part_III#Cases (last updated Aug. 4, 2016).

59 Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2012–2013 13, ¶ 4.13 (2013), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246455/0577.pdf; Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2013–2014 14, ¶ 4.13 (2014), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/350857/Annual-Report-of-the-Chief-Surveillance-Commissioner-for-2013-2014-laid-4-September-2014.pdf; *see also* Christopher Williams, *Two Convicted for Refusal to Decrypt Data,* The Register (Aug. 11, 2009, 1:17 PM), http://www.theregister.co.uk/2009/08/11/ripa_iii_figures/ (describing early prosecutions and convictions).

60 Investigatory Powers Act 2016, c. 25 (U.K.), http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf.

61 The United Kingdom previously tried to update its surveillance authorities with the Communications Data Bill of 2012. After the Liberal Democrats blocked the bill, then-Home Secretary Theresa May introduced a new version in November 2015. The Conservative government managed to enact the legislation before another major surveillance statute—the Data Retention and Investigatory Powers Act 2014—expired at the end of December 2016. To track how the Investigatory Powers Bill progressed through Parliament, see *Investigatory Powers Act 2016,* Parliament.uk, http://services.parliament.uk/bills/2015-16/investigatorypowers.html (last visited July 15, 2016).

62 For context on the new law and an early analysis of the draft legislation, see Daniel Severson, *Taking Stock of the Snoopers' Charter: The U.K.'s Investigatory Powers Bill,* Lawfare (Mar. 14, 2016, 12:17 PM), https://www.lawfareblog.com/taking-stock-snoopers-charter-uks-investigatory-powers-bill.

63 Investigatory Powers Act 2016 Explanatory Notes: Legal Background ¶ 22, http://www.legislation.gov.uk/ukpga/2016/25/notes/division/4/index.htm.

64 Investigatory Powers Act 2016, c. 25, § 229(3)(e) (U.K.).

65 *Id.* § 233 (4) (a).

66 *Id.* § 271(1), Schedule 10 (46) (2); *see also id.* § 16 (defining secondary data).

67 Regulation of Investigatory Powers Act 2000, c. 23, § 49(1)(a).

68 Investigatory Powers Act 2016, c. 25, § 253(1) (U.K.). The act defines "telecommunications operators" broadly to include service providers that facilitate the "transmission of communications by any means involving the use of electrical or electromagnetic energy." Id. § 261(13); *see also* id. § 261(10)-(12).

69 *Id.* § 253(5).

70 *Id.* § 253(6).

71 *Id.* § 253(1).

72 *Id.* § 255(3).

73 *Id.* § 253(8).

74 *Id.* § 253(7).

75 *E.g.*, Apple Written Evidence, IPB0093 (Dec. 31, 2016), http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26341.html ("We believe it would be wrong to weaken security for hundreds of millions of law-abiding customers so that it will also be weaker for the very few who pose a threat. In this rapidly-evolving cyber-threat environment, companies should remain free to implement strong encryption to protect customers.").

76 Joint Committee Report on the Draft Investigatory Powers Bill, HL Paper 93, HC 651 79 (2016), https://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf.

77 Home Department, Investigatory Powers Bill: Government Response to Pre-legislative Scrutiny, Cm 9219 40–41 (2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504174/54575_Cm_9219_WEB.PDF.

78 Home Office, Interception of Communications: Draft Code of Practice 59 ¶ 8.4 (2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/561091/16-10-18_Interception_code_of_practice_draft.pdf.

79 Investigatory Powers Act 2016, c. 25, § 255(3) (U.K.).

80 *See* Draft Investigatory Powers Bill November 2015, § 190(3) (U.K.), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf.

81 *See* Daniel J. Weitzner, *The Encryption Debate Enters Phase Two,* Lawfare (Mar. 16, 2016, 12:13 PM), https://www.lawfareblog.com/encryption-debate-enters-phase-two.

82 Investigatory Powers Act 2016, c. 25, § 2(2)(c) (U.K.).

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

84 *See* Philip Le Riche, *The Investigatory Powers Bill—It's Time to Take a Closer Look,* Graham Cluley (Mar. 22, 2016, 10:19 AM), https://www.grahamcluley.com/2016/03/investigatory-powers-closer-look/.

85 *Investigatory Powers Bill: Fact Sheets,* Gov.uk, https://www.gov.uk/government/publications/investigatory-powers-bill-fact-sheets (last updated July 8, 2016) (last visited Feb. 6, 2017).

86 Fact Sheet, Investigatory Powers Bill: Obligations on Communications Service Providers (CSPs), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/530557/Obligations_on_CSPs_Factsheet.pdf.

87 Regulation of Investigatory Powers Act 2000, c. 23, § 49(1) (U.K.).

88 *See* Fact Sheet, Investigatory Powers Bill: Obligations on Communications Service Providers (CSPs), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/530557/Obligations_on_CSPs_Factsheet.pdf.

89 Investigatory Powers Act 2016, c. 25, § 253(7) (U.K.).

90 *Id.* § 252(2)-(3).

91 Fact Sheet, Investigatory Powers Bill: Obligations on Communications Service Providers (CSPs), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/530557/Obligations_on_CSPs_Factsheet.pdf.

92 Investigatory Powers Act 2016, c. 25, § 252(5) (U.K.).

93 Letter from G.A. Van der Steur, Minister of Security and Justice, and H.G.J. Kamp, Minister of Economic Affairs, to the President of the House of Representatives of the States General regarding the Cabinet's View on Encryption, No. 708641 (Jan. 4, 2016) (English translation), https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on-encryption.

94 *See id.*

95 *Id.*

96 *Id.*

97 *Id.*

98 *Id.*

99 *See, e.g.*, *Dutch Government Says No to "Encryption Backdoors,"* BBC News (Jan. 7, 2016), www.bbc.com/news/technology-35251429.

100 Intelligence and Security Services Act 2002, arts. 24–25 (Neth.), https://fas.org/irp/world/netherlands/intel-act-2002.doc (unofficial English translation).

101 *Id.* arts 24(3), 25(7).

102 Wetboek van Strafvordering (Code of Criminal Procedure), § 126m(6) (Neth. 2012), http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafvordering_ENG_PV.pdf (unofficial English translation).

103 Letter from G.A. Van der Steur, Minister of Security and Justice, and H.G.J. Kamp, Minister of Economic Affairs, to the President of the House of Representatives of the States General regarding the Cabinet's View on Encryption, No. 708641 (Jan. 4, 2016) (English translation), https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on-encryption.

104 Jozsef Antal, *Hungary Introduces New Surveillance and Encryption Regulations Affecting Online Communications,* B:Inform (July 15, 2016), http://www.bakerinform.com/home/2016/7/15/hungary-introduces-new-surveillance-and-encryption-regulatons-affecting-online-communications.

105 *Id.*

106 *See* Christian Keszthelyi, *Hungarian Legislation Enables Encrypted Communication,* Budapest Bus. J. (May 12, 2016, 1:14 PM), http://bbj.hu/politics/hungarian-legislation-enables-encrypted-communication_116019.

107 *Id.*

108 Christian Keszhelyi, *Report: Government Could Ban Encrypted Messaging,* Budapest Bus. J. (Apr. 1, 2016, 9:20 AM), http://bbj.hu/politics/report-government-could-ban-encrypted-messaging_113840.

109 Dariusz Czuchaj, *Poland: The New Polish Surveillance Act—Back Door for Law Enforcement,* Mondaq (Mar. 11, 2016), https://www.mondaq.com/x/473658/Data+Protection+Privacy/The+New+Polish+Surveillance+Act+Back+Door+For+Law+Enforcement.

110 *See* Council of the European Union, Poland, Encryption of Data—Questionnaire (Sept. 20, 2016), https://www.asktheeu.org/en/request/3347/response/11727/attach/html/12/Encryption%20questionnaire%20PL.pdf.html.

111 *Id.*

112 *See* Catherine Stupp, *Five Member States Want EU-wide Laws on Encryption,* EurActiv (Nov. 22, 2016), https://www.euractiv.com/section/social-europe-jobs/news/five-member-states-want-eu-wide-laws-on-encryption/.

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

114 *See, e.g.*, Compliance with Court Orders Act ("Burr-Feinstein Bill"), S. ___, 114th Cong. (2014), http://www.burr.senate.gov/imo/media/doc/BAG16460.pdf.

115 28 U.S.C. § 1651.

116 For a discussion of this right in encryption cases, see Brendan M. Palfreyman, *Lessons from the British and American Approaches to Compelled Decryption,* 75 Brook. L. Rev. 345, 353–56 (2009). For a recent case analyzing this issue, see *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011,* 670 F.3d 1335 (11th Cir. 2012) (holding that act of decrypting and producing contents on hard drives is "testimony" within the meaning of the Fifth Amendment).

117 Note that Russia has taken perhaps the most extreme legislative action. The so-called Yarovaya Law requires internet service providers to hand over decryption keys, and an administrative statute reportedly restricts permissible types of encryption for internet traffic, thus enabling Russia's security services to prohibit any means of encryption that they cannot decrypt. *See* Scott Shackelford et al., *Decrypting the Global Encryption Debate,* Huffington Post (Oct. 20, 2016, 10:32 a.m.), http://www.huffingtonpost.com/entry/5808d3f9e4b00483d3b5d0bf.

118 Robert Hannigan, Director GCHQ, Front Doors and Strong Locks: Encryption, Privacy, and Intelligence Gathering in the Digital Era, Speech at MIT (Mar. 8, 2016), https://www.gchq.gov.uk/speech/front-doors-and-strong-locks-encryption-privacy-and-intelligence-gathering-digital-era. In a recent speech, European Commission Vice President Andrus Ansip also argued against back doors: "So-called 'backdoors to Internet' may sound tempting to ensure security, but would ultimately erode trust . . . and undermine the growth potential of the wider economy." European Commission, Speech by Vice-President Ansip at the High-level Conference on Protecting Online Privacy (European Pariament LIBE Committee) (Dec. 8, 2015), https://ec.europa.eu/commission/2014-2019/ansip/announcements/speech-vice-president-ansip-high-level-conference-protecting-online-privacy-european-parliament-libe_en.

119 *See Israeli Firm 'Helped FBI Crack San Bernardino Gunman's Cell Phone Without Apple's Help,'* Daily Mail (Mar. 30, 2016, 3:53 AM), https://www.dailymail.co.uk/news/article-3514875/Israeli-firm-helped-FBI-crack-San-Bernardino-gunman-s-cellphone-without-Apple-s-help.html.

120 *See* Palfreyman, *supra* note 116, at 373.

The preferred citation for this Publication is: Daniel Severson, ***The Encryption Debate in Europe,*** Jean Perkins Foundation Working Group on National Security, Technology, and Law (Hoover Institution), Aegis Series Paper No. 1702 (March 21, 2017), available at https://lawfareblog.com/encryption-debate-europe.

About the Author

DANIEL SEVERSON

Daniel Severson is a Harvard Law School and Harvard Kennedy School graduate. He served as editor-in-chief of the *Harvard International Law Journal* and writes for *Lawfare*. Daniel was a Harvard University Presidential Public Service Fellow at the Defense Department, a Council of American Ambassadors Fellow at the State Department, and a Fulbright Scholar in Taiwan. He plays the French horn.

Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cyber security, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The working group's output, which includes the Aegis Paper Series, is also published on the *Lawfare* blog channel, "Aegis: Security Policy in Depth," in partnership with the Hoover Institution.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200