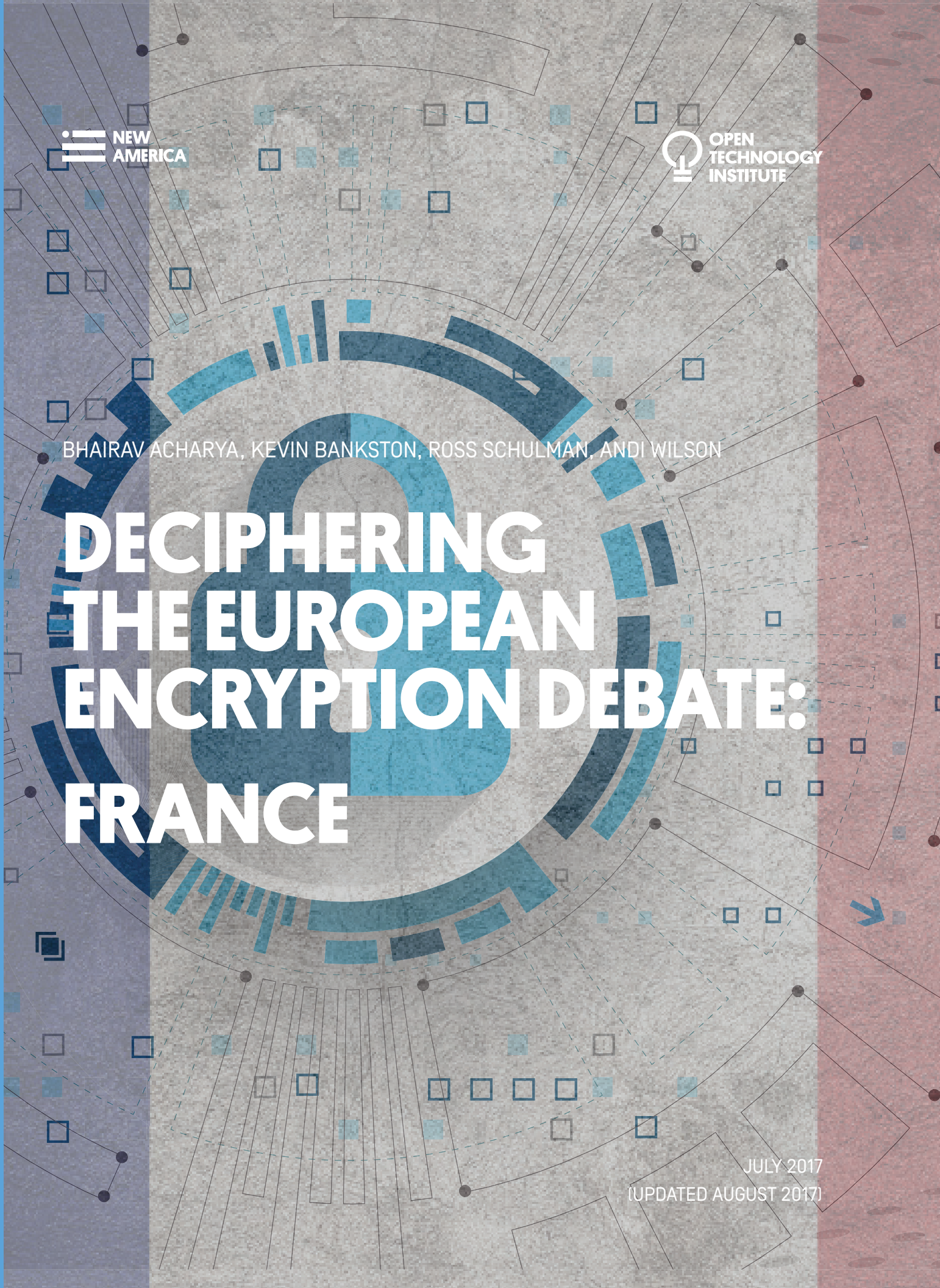

BHAIRAV ACHARYA, KEVIN BANKSTON, ROSS SCHULMAN, ANDI WILSON

DECIPHERING THE EUROPEAN ENCRYPTION DEBATE: FRANCE

JULY 2017
(UPDATED AUGUST 2017)

About the Authors

Bhairav Acharya is a lawyer and policy specialist interested in privacy, technology, freedom of expression, and the internet. He is a graduate of the National Law School of India University, Bangalore, and the University of California, Berkeley.

Kevin Bankston is the Director of New America's Open Technology Institute, where he works to ensure universal access to communications technologies that are both open and secure. He has previously worked as a digital rights attorney at the Electronic Frontier Foundation, the Center for Democracy & Technology, and the ACLU.

Ross Schulman is a co-director of the Cybersecurity Initiative and senior policy counsel at New America's Open Technology Institute, where he focuses on cybersecurity, encryption, surveillance, and internet governance. Prior to joining OTI, Ross worked for Google. He has also worked at the Computer and Communications Industry Association, the Center for Democracy & Technology, and on Capitol Hill. Ross earned his juris doctor magna cum laude from Washington College of Law at American University and his bachelor's degree in computer science from Brandeis University.

Andi Wilson is policy analyst at the Open Technology Institute where she focuses on issues including vulnerabilities equities, encryption, surveillance, and internet freedom. Before joining OTI, Andi received a Master of Global Affairs degree through the Munk School at the University of Toronto. Andi also worked on political affairs and international security at the Embassy of Canada in Bangkok, Thailand.

Acknowledgements

The authors would like to thank Bertrand de La Chapelle, Félix Tréguer, and Le Quadrature du Net for their comments and assistance on this paper. This paper does not necessarily reflect their views. As well, we appreciate the extensive help of New America's staff and fellows for their support on this project.

About New America

New America is committed to renewing American politics, prosperity, and purpose in the Digital Age. We generate big ideas, bridge the gap between technology and policy, and curate broad public conversation. We combine the best of a policy research institute, technology laboratory, public forum, media platform, and a venture capital fund for ideas. We are a distinctive community of thinkers, writers, researchers, technologists, and community activists who believe deeply in the possibility of American renewal.

Find out more at **newamerica.org/our-story**.

About OTI

The Open Technology Institute (OTI) works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Find out more at **www.newamerica.org/oti**.

About this Series

The right to use strong encryption technology—like the encryption that secures your iPhone or protects your Whatsapp messages—isn't only under political attack in the United States.[1] Governments in the United Kingdom,[2] Germany,[3] France,[4] and other European countries[5] have recently taken steps toward undermining encryption. In particular, a range of government stakeholders have been pressing for service providers to re-engineer their encrypted products so that they always hold a key to their users' data—often referred to as a "key escrow" scheme, or "exceptional access," or a "backdoor"—or to simply not offer such products at all.

Although these local debates have engaged a wide range of policymakers, privacy advocates, and internet companies, they've been taking place largely in isolation from each other, with limited sharing of information, arguments, and advocacy tactics between those countries' policy communities. These papers will fill in some of those gaps by mapping the legal landscape and political dynamics around encryption in various European capitals. This is the third of these papers, focused on the encryption debate in France. The other papers in the series cover the encryption debates in Germany and the United Kingdom.

Contents

Introduction	2
Current Legal Landscape: No Clear Backdoor Mandate...Yet	3
The French Encryption Debate: From Parliament to President	5
Lessons Learned and Strategies for Action	12
Notes	14

INTRODUCTION

The political landscape in France is worrisomely ripe for the enactment of new laws or policies that could undermine the security of encrypted products and services in the name of national security. Since the tragic November 2015 terrorist attacks in Paris, France has been in a state of emergency that has been renewed five times in the face of continuing terror incidents.[6] During this period, in 2015 and 2016, the French Parliament aggressively expanded the government's surveillance and lawful hacking authorities,[7] expanded penalties for failure to comply with an existing law allowing for compelled key disclosure in criminal investigations,[8] and created a new mandatory key disclosure and decryption authority for use in intelligence investigations.[9] However, French lawmakers have not (yet) passed any law that would clearly require providers of encrypted products and services to redesign their secure services to ensure government access on demand, which would effectively ban strong encryption products without "backdoors" for surveillance.

However, the French Parliament came dangerously close to passing a backdoor mandate in 2016 as it debated a range of anti-encryption proposals, including one that failed by only one vote in the National Assembly.[10] Bills that could have mandated backdoors—supported by a David vs. Goliath narrative where France stands up to the massive Silicon Valley companies that put their profits ahead of France's security—were headed off in part by the interventions of key leaders in the Socialist Party which controlled the government at the time.[11] But times are changing. Now, France has a new president, Emmanuel Macron, who has taken an aggressive stance on encryption and allied himself with U.K. Prime Minister Theresa May, another hawk on the issue.[12] Meanwhile, French law enforcement officials continue their multi-year push—including in the *New York Times*[13] and at the EU level[14]—for legislation that would ensure that they can always obtain the encrypted data they seek. Under these conditions, it seems that the encryption debate in France is just beginning—and could end abruptly in favor of backdoors in the face of another major terror attack.

The French Parliament came dangerously close to passing a backdoor mandate in 2016 as it debated a range of anti-encryption proposals, including one that failed by only one vote in the National Assembly.

CURRENT LEGAL LANDSCAPE: NO CLEAR BACKDOOR MANDATE...YET

Encryption

France has no law that explicitly allows the government to compel companies to redesign their encrypted products or services to facilitate government access (i.e., to demand "backdoors"). As described below, however, there are multiple legal provisions spread across the Criminal Procedure Code, the Penal Code, and the Internal Security Code—some pre-dating the latest terrorist attacks and others passed in legislation responding to those attacks—that may be used to compel the disclosure of encryption keys in a company's possession or the decryption of data.[15] Although some of those provisions are worded broadly enough that the government might attempt to use them to compel a backdoor, there are no known instances of any such attempts, and failed legislative efforts in 2016 to pass an explicit backdoor mandate indicate that at least some policymakers believe that current laws are not so broad.[16]

Starting with the Criminal Procedure Code, Articles 60-1 and 60-2 contain broad language that allows judges to order individuals and companies to hand over information needed for criminal investigations. Under Article 60-1, a judge can order the disclosure of information "relevant to [an] inquiry" to law enforcement agencies regardless of whether the information is legally privileged,[17] while under Article 60-2, a judge can order the disclosure of "information necessary for the discovery of the truth," but legally privileged information is exempted; refusal to comply with either can be punished with fines of 3,750 euros.[18] While neither provision specifically addresses encryption, the added context of the legislative debates of 2016—described at length on the next several pages—provides some indication that legislators believe these provisions might be used, for example, to demand that a smartphone provider be able to disclose a smartphone user's encrypted data.

Another provision of the Criminal Procedure Code, Article 230-1, imposes a duty on anyone the government sees fit to command "to carry out the technical operations necessary to obtain a readable version of [requested] information, and also, where a method of encryption has been used, the secret key for decoding it," although the penalties for disobeying such a command are not specified in the article.[19] When it comes to encryption, this technical assistance provision on its face only seems to apply where the person ordered to provide the requested data actually possesses the encryption key—or at least is silent about what happens if that person doesn't have the key—rather than clearly

demanding that any provider of encryption always maintain a key to enable decryption.

The French Penal Code contains a similar encryption-specific provision. Article 434-15-2, which addresses "Obstacles to the Exercise of Justice," provides that "anyone who, having the key to decipher an encrypted message which may have been used to prepare, facilitate or commit a felony or a misdemeanour refuses to disclose that key to the judicial authorities or to operate it following instructions issued by the judicial authorities" faces three years imprisonment and a fine of 270,000 euros. The same article increases penalties to 450,000 euros if the refusal deprives the government of evidence that could have prevented a crime or diminished its effect.[20] This article was created in 2001, but was amended by the Organized Crime and Terrorism Act of 2016 to make the penalties even harsher.[21] Although that amendment occurred in the context of the French legislature debating the issue of encryption while watching the U.S. legal controversy between the Federal Bureau of Investigation (FBI) and Apple over iPhone encryption play out, this provision notably does not appear on its face to provide authority for any kind of technical mandate as was considered in that case, since it only applies to parties that actually possess the necessary keys.

Finally, Article L871-1 of the Internal Security Code, which was enacted by the Intelligence Act of 2015, gives the prime minister the power to order "entities that provide cryptographic services intended to ensure privacy" to hand over information necessary "to decipher data" to intelligence agencies.[22] The prime minister can also order the same entities to decrypt the data themselves. Recipients of such orders must obey within 72 hours, and failure to comply could lead to two years imprisonment and a 150,000 euro fine.[23] However, the section provides the opportunity for the recipient to show that they are unable to comply, a provision that providers could presumably avail themselves of if the design of their product did not enable them to decrypt their users' data.[24]

Government Hacking

While a number of the provisions in French law dealing with encryption date back to the turn of the century, France has only much more recently begun legislating around the issue of hacking by the government for criminal or intelligence investigations.[25] The first provisions for government hacking in France were enacted in 2011, as part of the wide-ranging Law on the Orientation and Programming for Internal Security (LOPPSI 2).[26*] Included in its long list of provisions was authorization for the French authorities to use malware in the course of their investigations.[27] The 2011 law created Articles 706-102-1 through 706-102-9 of the Code of Criminal Procedure, which authorize certain government agents to place "technical devices" without the consent of the owner of the target equipment. The Organized Crime and Terrorism Act of 2016 amended most of those articles to clarify and further provide for judicial authorization of surreptitious remote hacking in criminal investigations. These provisions, which provide for authorization either by the judge of freedoms and detention (*le juge des libertés et de la détention*) or the investigating judge in regard to a specific list of serious crimes, allow for either remote access initiated by the physical installation of software (such as a keylogger) on the target computer, or remote access that is also initiated remotely.[28] The articles also prescribe limits on the use of the hacking power, including time limits of either two or four months depending on who authorized the intrusion, a requirement of particularity regarding what data may be searched for, and a requirement that the seized data be destroyed after the investigation and prosecution concludes.[29]

Moving from law enforcement to intelligence investigations, the prime minister can authorize the intelligence services to hack into computers under Article L853-2 of the Internal Security Code, which was established by the Intelligence Act of 2015.[30] Before the prime minister can issue an authorization, there must be a written and reasoned request for hacking by a senior cabinet

minister.[31] The prime minister's authorization must be made in consultation with the National Oversight Commission for Intelligence-Gathering Techniques (CNCTR), an independent body made up of lawmakers, judges, and technical experts.[32] The prime minister is not bound by the advice of the CNCTR, but where the prime minister acts in contravention of that advice, the hacking authorization may be challenged in the *Conseil d'Etat*, France's highest court for administrative matters.[33]

Hacking by French intelligence agencies almost certainly took place with regularity before the 2015 amendments. French malware has been found on systems around the world since at least 2007.[34] Intelligence services are not generally talkative about their abilities, but public reporting has characterized some of their malware as capable of intercepting traffic from Skype or Facebook, as well as keystroke logging.[35] In contrast to the intelligence services, however, hacking for law enforcement purposes is still quite rare in France despite the law providing for it, in part because French judges and prosecutors lack access to appropriate hacking tools and techniques and lack the knowledge to use them effectively even if they did have access.[36] This may be a part of the explanation for why there has been so much emphasis on legislative debate over backdoors in France, to which we turn in the next section—hacking is not yet considered a viable alternative method for obtaining encrypted data as it is, for example, in Germany.[37]

THE FRENCH ENCRYPTION DEBATE: FROM PARLIAMENT TO PRESIDENT

In 2016, the debate over encryption and backdoors landed squarely in the French legislature, as the bounds of technical assistance that tech companies must provide to law enforcement and the penalties for failing to provide that assistance took center stage.

In particular, encryption was the focus of five major amendments that were proposed in the context of two pieces of legislation: the Digital Republic Act and the aforementioned Organized Crime and Terrorism Act.[38] After spirited debate that often but not always broke down across party lines—with the conservative opposition pushing for anti-encryption legislation and the majority socialist government pushing back—all but one of those amendments were defeated in the Assembly. The one amendment that did pass—an amendment to the crime and terrorism bill that increased penalties for failure to hand over encrypted data when required under existing law[39]—was ultimately stripped out by the Senate, but then replaced with a similar penalty enhancement for a different but similar provision of existing law.[40]

In a worrisome sign for the future, several of the rejected amendments, including one that was narrowly defeated by only one vote, would have clearly required providers to design their products so as to maintain the capability to decrypt their users' data on command—essentially, a backdoor mandate requiring that providers not offer encryption for which they don't also have the keys.[41] The first of those backdoor amendments, some version of which one could imagine being re-introduced with the new president's support in the wake of a new major terror attack, was proposed in the debate over the Digital Republic Act, to which we turn next.

The Digital Republic Act: The Backdoor Debate Begins

In January 2016, the National Assembly was debating the bill that would become the Digital Republic Act, which included a range of new rules for data privacy, net neutrality, and other aspects of France's digital economy.[42] In the context of that debate, Deputy Nathalie Kosciusko-Morizet, a senior member of the most powerful conservative party, the Republicans (*Les Républicains*), brought an amendment demanding that "[m]anufacturers of equipment must take into account in their design the need to give law enforcement authorities, in the context of a judicial inquiry and after the authorization of a judge, access to the requested materials," and authorizing the Council of State—a governmental body that serves as legal advisor to the Executive Branch—to lay down detailed rules implementing this requirement.[43] Kosciusko-Morizet's proposal was supported by Deputies Philippe Gosselin and Lionel Tardy, both members of the center-right Union for a Popular Movement party (*Union pour un mouvement populaire*).[44]

As the summary statement in the amendment made clear, it was intended to "open the debate on ways and means of ensuring access to data for reasons of national security and in the context of a judicial inquiry."[45] Her amendment also aimed to address the problem posed by the increasing move toward encrypted communications, saying that while encryption may help ensure the security of personal data it also poses a problem for government investigators. Kosciusko-Morizet echoed this sentiment in the debate, noting that "these [encrypted] devices, which multiply in response to [surveillance] scandals…have their utility; but they can…become a barrier to security services."[46] She was quick to defend the proposal as narrowly targeted: "I am not proposing permanent access to [encrypted devices]…[only] the possibility for the services to have access to the data they need quickly."[47] However, this straw-man argument—no one in the debate over backdoors has claimed that governments are seeking permanent or unchecked access to devices—echoes defenses offered by officials in other countries who have said they don't want a backdoor while specifically demanding the redesign of encrypted products to introduce new access mechanisms to facilitate government access. A quintessential example is former FBI director James Comey who said that the special access mechanism he was seeking wasn't a backdoor but a "front door," since it would only be used with a court's approval.[48]

Deputy Axelle Lemaire, the highly-regarded digital affairs minister of the Socialist Party (*Parti Socialiste*) that held the majority and the presidency at the time, was not fooled by such word-games and dismissed the Kosciusko-Morizet proposal as "a vulnerability by design."[49] Mandatory backdoors, she argued, would open "the door to actors who pursue less than noble intentions, not to mention the economic damage suffered by the companies and their customers…[I]n the Government's view, systematically [weakening cybersecurity] is not the correct answer to the problem."[50] Lemaire explained that encryption backdoors are a harmful policy approach because they create network vulnerabilities which could be exploited by actors other than the government, using as an example the recent Juniper Networks scandal where "unauthorized code" for electronic eavesdropping was discovered in Juniper's Virtual Private Network software.[51] "[An encryption] backdoor…hurt[s] the whole community, since personal data is no longer protected at all," she said.[52] Isabelle Attard from the

progressive-left New Deal party (*Nouvelle Donne*) supported Lemaire's stand, arguing that demanding backdoors into digital devices was akin to requiring that "every building should have a backdoor in case of possible intervention by law enforcement, which could be much more often used by ill-intentioned persons."[53]

In the face of broad opposition, Kosciusko-Morizet withdrew her amendment,[54] but the debate over encryption was far from over: four more anti-encryption proposals were soon being debated in the context of the Organized Crime and Terrorism Act of 2016.

The Organized Crime and Terrorism Act of 2016: Four More Anti-Encryption Proposals

In the spring of 2016, while the dispute between Apple and the FBI over access to devices with full disk encryption played out in the United States, French legislators were debating changes to their own laws around encryption and the technical assistance obligations of tech companies.[55] In particular, as France's parliament was considering the Bill to Combat Organized Crime and Terrorism,[56] which would enhance the government's investigative, surveillance, and hacking powers in a variety of ways, legislators in the Assembly proposed four different amendments that addressed encryption. Although only one of them passed the Assembly and was then replaced by the Senate with a different but similar provision in the final bill, the legislative debate over those four amendments—to which we turn next—is illustrative of the current state of the encryption controversy in France. The overriding theme of that debate: France as David and the U.S. tech industry as Goliath in a fight over French security versus American profit.

1. The Goujon Amendment: Decrypt or Go to Prison

A group of National Assembly legislators from the two center-right parties, led by Deputy Philippe Goujon of the Republicans, introduced the one anti-encryption amendment that would ultimately survive the Assembly vote and go to the Senate. The Goujon proposal would have amended Articles 60-1, 60-2, and 230-1 of the already existing Criminal Procedure Code, which were described earlier in this paper—that is, the two general provisions regarding production of information relevant or necessary to a criminal case, and the provision regarding technical assistance and encryption key disclosure.[57] In particular, the amendment threatened to severely enhance the penalties for failing to comply with demands under those code provisions in cases related to terrorism, even more so in cases where "a private body refuses to communicate to the requesting judicial authority investigating terrorist offenses…[the requested] data protected by a cryptological means of which it is the manufacturer."[58] In other words: if your company can't provide decrypted data on demand, it should be prepared to face a 350,000 euro fine.[59] More than that, the amendment went so far as to provide for five years of prison for the individuals—such as company executives—that fail to comply.[60] Goujon argued that the amendment was needed because the existing penalties, which had never been invoked before, were "derisory,"[61] and he maintained that punishing employees was a useful and reasonable way of punishing companies.[62]

Deputy Pascal Popelin of the majority, center-left Socialist Party was only cautiously supportive when his views were sought. He said, "We all agree that strengthening the penalties [for refusing] to cooperate with [lawful orders] is one of the best means of [securing access to] information," but he did not support punishing employees.[63] Deputy Éric Ciotti, a Republican that cosponsored the amendment with Goujon, in turn accused Popelin of succumbing to "fear that has prevented you from taking necessary measures against these [Silicon Valley] giants who refuse to cooperate with [French authorities] and terrorize you…"[64] Casting the U.S. tech industry as the villain that was trading on the security of the French people in pursuit of profit was and is a common theme in the French encryption debate.

Ciotti's nationalist rhetoric was successful; Goujon's amendment was adopted by the National Assembly. However, the Senate Committee of Laws stripped

the amendment out of the bill and replaced it with a much more modest change to the law.[65] Rather than adding new language specifically targeted at manufacturers of encrypted products, the Senate simply increased the penalties for the existing versions of Article 60-1 and 435-15-2 of the Criminal Code (thereby avoiding any substantive change in what those laws require). And instead of a fine of 350,000 euros for failing to hand over encryption keys as the Assembly had intended, the final version of the law that passed the Senate only upped the penalty to 150,000 euros (which was still a six-fold increase over the existing law). The Senate Committee also rejected the idea of prison sentences for individual company employees, noting that "[I]t appears disproportionate…to provide for prison sentences [for employees]. Moreover, these penalties are essentially aimed at legal persons, manufacturers or suppliers of cryptographic means or encryption keys, [not at actual people]."[66] The Senate also noted that Article 434-15-2 of the Penal Code already punished refusals to cooperate. Therefore, the Senate found Goujon's amendment "superfluous and counterproductive."[67]

By rejecting the Goujon amendment's targeting of encryption providers, the Senate headed off what could have amounted to a backdoor mandate. However, Goujon was not the only lawmaker to pose such a threat. Nor were only Republican legislators pushing backdoor amendments, as the next example demonstrates.

2. The Galut Amendments: No Backdoor? Pay a Million Euros

Deputy Yann Galut of the Socialist Party, supported by a large group of Socialists and members of smaller left-wing parties, also proposed two encryption-related amendments to the Bill to Combat Organized Crime and Terrorism, amendments drafted broadly enough to potentially require companies to design backdoors into their products or face serious financial consequences.[68] In particular, both amendments would have created new articles in the Code of Criminal Procedure authorizing legal demands to require that "a designer of electronic equipment access, by any means, data likely to be of interest to the current investigation that is contained in electronics of its design"—with a massive one million euro fine for failure to comply.[69] The difference between the amendments was in who could issue one of these demands. In one version, the order could come from investigating judges or their designees; in the other version, a prosecutor could issue the order after approval by a judge of freedoms and detention.[70] In France's judicial system, investigating judges are independent magistrates who proactively investigate crimes with the help of the police, whereas the freedom and detention judges oversee detention orders and a number of other related magistrate functions. Galut argued that his amendment was necessary based on the claim that "dozens of terrorism-related investigations are blocked because smartphone manufacturers have decided…to completely block access to telephones and, moreover, the [encryption] key."[71] He also cited, in support of his amendment, an August 2015 *New York Times* op-ed from Manhattan district attorney Cyrus R. Vance Jr. and Paris Chief Prosecutor Francois Molins arguing that phone encryption was obstructing justice.[72]

Like Goujon and Ciotti, Galut also used a David and Goliath argument to push his amendment. "We are faced with the willingness of multinationals to ensure that judicial investigations fail because they have decided to do so. It is unacceptable! … We cannot accept that the law of the strongest, the law of money, reigns above all in the so-called name of freedom. In the name of freedom, we must find a technical solution to compel [Silicon Valley companies]!"[73] Galut further argued that qualified access to certain devices and communications in specific conditions did not deviate from accepted legal principles (while ignoring the security risks that such access mechanisms would create): "I do not understand [how] the defenders of freedoms… can oppose the search of a laptop when a house or a car can be searched!"[74] Popelin, who had been ambivalent about the Republican proposals, agreed vigorously with Galut. "I adhere to the… explanations given by Yann Galut [and agree that]

we [should] no longer be confronted with this type of blocking in the name of a pseudo-defense of freedoms."[75]

However, other lawmakers called out and critiqued the jingoistic David and Goliath narrative being spun by the amendments' supporters. For example, Sergio Coronado from the Green Party (*Europe Écologie Les Verts*) expressed concern that other legislators were oversimplifying the debate by framing it as a binary fight against large multinationals rather than a challenging question of how best to maintain the freedoms and security of the French people; he further noted that by deploying encryption Apple was responding to the security concerns of customers in the face of widespread reports of mass surveillance, a reference to the NSA spying revealed by Edward Snowden.[76] "The subject is much more complex. I am very surprised that some parliamentarians present it in such a binary way...There are not, on the one hand, multinationals totally insensitive to terrorist violence, and on the other, judges solely attached to the discovery of the truth!"[77]

Republican Deputy Thierry Mariani also sought to highlight the complexity of the issue, pointing out that the providers of communications and encryption services were not solely located in the United States: "[T]he problem today is no longer Apple or Google: it is Huawei in China, or Samsung in Korea. What then? Run continuously after each producer? Perhaps we will be able to speak with American companies, which operate in a legal system that we know, but how will we impose ourselves against Huawei, a Chinese company that will definitely overtake Apple in a few years?"[78]

The French Justice Minister Jean-Jacques Urvoas echoed both Coronado and Mariani's arguments. "What is the origin of the problem? While it is true that these [Silicon Valley companies] are essentially driven by mercantile interests, the behavior of the NSA...led it to loot [private data] to the extent that everyone felt that it had to be stopped. The commercial response of these [companies] was to offer their customers the guarantee of not being spied on!"[79] He also made it clear that a French law alone would not solve the problem of access to encrypted data: "It should be noted that the Americans themselves are powerless, while their ability to influence [Silicon Valley] is far superior to ours...A national law is, in my view, inoperative. The answer lies in international cooperation." He went on to describe how he, the prime minister, and the interior minister had traveled to Brussels the previous month, February 2016, to "encourage the European Union to [take a common position on] these issues. I am fairly confident about the emergence of a common position at the level of the Union."[80] Shortly after these comments, the Assembly adjourned for 15 minutes, during which Urvoas conferred privately with his fellow Socialist Party member Galut. When debate resumed, Galut withdrew both his amendments based on his conversation with Urvoas and the assurance that the issue was being discussed at the EU level.[81]

3. The Ciotti Amendment: Locking Uncooperative Providers Out of the French Market

Justice Minister Urvoas was less successful at convincing Deputy Ciotti from withdrawing his own anti-encryption amendment to the crime and terrorism bill, which was on the table and being debated at the same time as Galut's amendments.[82] Ciotti's amendment would have created a new criminal provision requiring "manufacturers of telecommunications tools, telecommunications operators, [and] Internet service providers" to pay a fine of two million euros and face a one-year ban from the French market if they failed to "communicate all relevant information" to the French authorities in a terrorism investigation.[83] Ciotti said that such penalties were necessary to impact the behavior of Silicon Valley companies "with a market capitalization of several hundred billion dollars [that] consider states as dwarfs and despise laws," arguing that his amendment was necessary to protect the French people from "companies that place themselves above [France's] guarantees of freedom."[84] Ciotti brushed aside concerns that his amendment threatened security and the fundamental right to privacy: "The defense

of public freedoms cannot be used as an excuse for the development of practices that favor terrorism."[85] Echoing previous straw-man arguments around security concerns, he claimed that his amendment would not result in the "penetration of all mobile phones thanks to the so-called backdoor technique," which was not reassuring to those concerned.[86]

Members of the Assembly speaking in opposition generally agreed with the need for solutions, but thought that Ciotti's penalties were too extreme. Others, such as Deputy Cavard, worried that France compelling companies to undermine their encryption risked "paving the way" for other less savory countries to do the same.[87] Deputy Coronado echoed the sentiment: "Think about what could happen to decryption keys in the hands of authoritarian regimes, like China, North Korea, or Syria."[88] Some were also swayed by Justice Minister Urvoas' intervention seeking a more measured, EU-level conversation. In explaining his "no" vote, Deputy Tourret praised Urvoas' attention to the issue and said that he would follow Urvoas' decision not to vote for Ciotti's amendment.[89]

In the face of such opposition Ciotti's amendment was narrowly defeated—but only by one vote.[90]

The French Debate Goes International, and Presidential

As Justice Minister Urvoas had indicated during the legislative debate, by early 2016 the encryption debate was becoming an EU-wide issue, and by mid-2016 several top European law enforcement officers were agitating for a Europe-wide legislative solution to their encryption problem that sounded a lot like a backdoor mandate. That August, French Interior Minister Bernard Cazeneuve and German Interior Minister Thomas de Maizière jointly called on the EU to pass legislation to impose new obligations on communications providers to decrypt messages.[91] That call was reiterated in February 2017 in a joint letter to the European Commission from Maizière and from Bruno Le Roux, Cazeneuve's successor as the French Interior Minister.[92] These overtures by the interior minister are puzzling, considering that the governing Socialist party had stated in the context of the Digital Republic Act debate that it was opposed to backdoors. They may have signalled a shift in government policy, or—as we've seen in Germany and the United States—may have been unsanctioned departures from government policy by aggressive law enforcement leaders.

This question may be moot after the May 2017 presidential election, since the new president, Emmanuel Macron, has explicitly taken a much more aggressive stance against encryption than his predecessor. Echoing legislators that cast Silicon Valley as allies of terrorists and enemies of security, Macron tweeted during the campaign that "Internet actors," if they refused to help the government, should be considered complicit in terrorist attacks.[93] He went on to announce that if he was elected, "France [would] launch a major initiative beginning this summer 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."[94] Making good on that promise, he has since aligned himself on the issue with British Prime Minister Theresa May, herself an aggressive anti-encryption crusader.[95] Together with May, he announced in June 2017 a joint counter-terrorism action plan that included a call for greater access to online communications, saying that France was "committed to improve the means of access to encrypted content in conditions that preserve the confidentiality of messages."[96] In a joint "French-British Action Plan" released to the public, one of the three core goals was ensuring access to information in investigations.[97] "When encryption technologies are used by criminal groups, and terrorists," the leaders wrote, "it must be possible to access the content of communications and their metadata."[98] The document attempted to reassure the concerned that "[t]his is not about backdoors or banning encryption, but ensuring Governments and companies develop shared solutions to this issue."[99] However, such assurances are less than convincing considering that ensuring access to encrypted data in *all* cases—which is the stated goal—would necessarily require encryption backdoors or bans.

However, even if the new French president would support a backdoor mandate, other parts of his government may not. As in all of the other countries we've looked at, government stakeholders focused on data protection, cybersecurity, and the digital economy have been clear in their opposition to heavy-handed mandates against encryption providers. In France, at least two agencies in particular have expressed opposition to restrictions on encryption. The first is France's national data protection agency, the *Commission Nationale de l'informatique et des Libertés* (CNIL), or the National Commission on Informatics and Liberty. Ironically, the Digital Republic Act—which almost had a backdoor amendment attached to it—clarified and expanded CNIL's mission to include "promot[ing] the use of technologies that protect privacy, including data encryption technologies,"[100] and it has definitely done so. For example, in a statement from April 2016, it expressed the opinion that backdoors would create collective risk to individual security, and ultimately would not prevent criminals from using encryption to obscure their communications.[101] It also argued that backdoors would be targeted by state attackers and organized crime, and that they would be extremely complex to implement in a safe way.[102] The French Network and Information Security Agency (ANSSI), an inter-ministerial agency responsible for the government's cyber defense and reporting directly to the prime minister, has also expressed similar concerns about the insecurities created by backdoors, and issued a memo in 2017 supporting the use of robust encryption.[103]

There may even be key Macron advisors with a similar perspective on the importance of preserving strong encryption. For example, just after the election and in the wake of the release of emails stolen from the Macron campaign, Macron's then-digital advisor and current Secretary of State for Digital Affairs, Mounir Mahjoubi, tweeted that "[w]e need to cultivate a culture of encryption, of protection."

Similarly, there are strong voices at the EU level pushing back against anti-encryption proposals like those of the French and German interior ministers. Most notably, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) put forward an extensive digital privacy proposal in June 2017 that would amend the EU's Charter of Fundamental Rights to explicitly extend privacy rights to the digital realm. In particular and most relevant here, the proposal includes an express prohibition on backdoor mandates: "Member States shall not impose any obligations on electronic communications service providers that would result in the weakening of the security and encryption of their networks and services."[104]

In sum, although anti-encryption action in the French legislature is still a significant threat—likely all the greater after Macron's election—there continue to be components of the French government and European political society that would provide stiff opposition to any such effort. But will it be enough?

LESSONS LEARNED AND STRATEGIES FOR ACTION

Those who seek to defend encryption are facing a perfect storm in France, where:

- The country has faced sustained terror attacks over the past several years;
- The level of nationalist disdain for U.S. tech companies is the highest we've seen in any of the countries we've studied, feeding a dangerously simplistic David (France) vs. Goliath (Silicon Valley) narrative and blunting the impact of any lobbying by that sector;
- The modest local internet and tech industry has so far been unable or unwilling to take up the slack for the U.S. companies in making economic and technical arguments that might be persuasive to lawmakers eager to stick it to Silicon Valley;
- The new president appears aligned with top law enforcement officials in his desire for a national or EU-level law to ensure government access to any encrypted data the government seeks;
- There is a serious dearth of native civil society and computer security voices to push back on such plans relative to even Germany or the United Kingdom, much less the United States;
- Similarly, although there are some government agencies that have clearly opposed backdoors, there is not such a broad or powerful set of agencies taking that position as we have seen in, for example, the United States and Germany; and,
- Unlike in Germany and the United States where government hacking has been approached by many policymakers as a more reasonable alternative to demanding that providers weaken their secure products, France is still early in its development of investigative hacking capability such that this release valve in the backdoor debate is unavailable.

Therefore, and to avoid the passage of a backdoor mandate that could be the first domino in a wave of such mandates throughout the West, significant attention must be paid to the French encryption debate.

- Intense investment by philanthropic or corporate stakeholders is necessary to help support local civil society and tech voices to engage in the debate and short-circuit the David vs. Goliath narrative, and to provide for mutual support between civil society actors across borders. If the choice is between investing resources here or in the United Kingdom or

Germany, France definitely has the greatest need, and poses perhaps the gravest threat, considering that the United Kingdom has already passed the provisions of law that it is most likely to attempt to use as a backdoor mandate as part of its Investigatory Powers Act, while a legislative mandate in Germany appears very unlikely at this point. However, investment at the EU level in Brussels will also be critical.

- Considering that cybersecurity and economic arguments were the only ones that were persuasive in recent legislative debates (consistent with what we've seen in other countries), but also considering the difficulty in finding adequate local voices to make those arguments, it may be that a fruitful next step would be the development of a pan-European network of security and tech sector experts that could opine as a group both in France and elsewhere on the dangers of backdoors—in a way that cannot be dismissed as self-interested Silicon Valley lobbying.

- Building on current transatlantic dialogues between the United States and Germany that are seeking to develop alternatives to backdoors (including rights-protecting frameworks for government hacking), a concerted effort is required to broaden France's perspective on the range of lawful access strategies beyond backdoors that are available to its investigators in the twenty-first century. Without such alternatives, it may be impossible to ramp down the intense and growing pressure for backdoors in France.

Notes

1 Jason Koebler, "Could Anybody Be Worse Than James Comey On Encryption? We're About to Find Out," *Motherboard*, May 9, 2017, https://motherboard.vice.com/en_us/article/could-anybody-be-worse-than-comey-on-encryption-were-about-to-find-out.

2 Kieren McCarthy, "U.K.'s New Snoopers' Charter Just Passed an Encryption Backdoor Law by the Backdoor," *The Register*, November 30, 2016, https://www.theregister.co.uk/2016/11/30/investigatory_powers_act_backdoors.

3 Sven Herpig and Stefan Heumann, "Germany's Crypto Past and Hacking Future," *Lawfare*, April 13, 2017, https://www.lawfareblog.com/germanys-crypto-past-and-hacking-future.

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

5 Catherine Stupp, "Five Member States Want EU-wide Laws on Encryption," *Euractiv*, November 22, 2016, https://www.euractiv.com/section/social-europe-jobs/news/five-member-states-want-eu-wide-laws-on-encryption/.

6 Yasmeen Serhan, "Will France's State of Emergency Become Permanent?" *The Atlantic*, July 11, 2017, https://www.theatlantic.com/international/archive/2017/07/will-frances-state-of-emergency-become-permanent/532848/.

7 See generally LOI n° 2015-912 du 24 juillet 2015 relative au renseignement (1) [Law 2015-912 of July 24, 2015, Relating to Intelligence (1)] available at https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899; Internal Security Code, Art. L871-1. For the purposes of this paper this will be called the "Intelligence Act of 2015." and LOI n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale [Law 2016-731 of June 3 2016, Strengthening the Fight Against Organized Crime and Terrorism and Their Financing and Improving the Efficiency and Guarantees of Criminal Procedure] available at https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231&categorieLien=id. For the purposes of this paper this will be called the "Organized Crime and Terrorism Act of 2016"; see also Zone d'Intérêt, "A Look at the Latest French Laws on Intelligence Collection," February 26, 2016, https://zonedinteret.blogspot.de/2016/02/a-look-at-latest-french-laws-on.html; Aurelien Breeden, "French Authorities Given Broader Powers to Fight Terrorism," *New York Times*, May 25, 2016, sec. Europe, https://www.nytimes.com/2016/05/26/world/europe/france-terrorism-laws.html.

8 Code pénal [Penal Code], Art. 434-15-2

9 Code de la sécurité intérieure [Internal Security Code], Art. L871-1.

10 See generally "The Encryption Debate in France," 6; Daniel Severson, "Encryption Legislation Advances in France," *Lawfare*, April 14, 2016, https://www.lawfareblog.com/encryption-legislation-advances-france.

11 Ibid.

12 Bhairav Acharya, Kevin Bankston, Ross Schulman and Andi Wilson, "Deciphering the European Encryption Debate: United Kingdom," New America's Open Technology Institute, June 2017, available at https://www.newamerica.org/oti/policy-papers/deciphering-european-encryption-debate-united-kingdom/.

13 Cyrus R. Vance Jr., Francois Molins, Adrian Leppard and Javier Zaragoza, "When Phone Encryption Blocks Justice," *New York Times*, August 11, 2015, https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html.

14 Iain Thomson, "Germany, France Lobby Hard for Terror Busting Encryption Backdoors – Europe Seems to Agree," *The Register*, February 28, 2017, https://www.theregister.co.uk/2017/02/28/german_french_ministers_breaking_encryption/.

15 Criminal Procedure Code, Arts. 60-1, 60-2, 230-1; Penal Code, Art. 434-15-2; Internal Security Code, Art. L871-1.

16 "The Encryption Debate in France," 6.

17 Criminal Procedure Code, Art. 60-1.

18 Ibid., Art. 60-2.

19 Ibid., Art. 230-1.

20 Penal Code, Art. 434-15-2.

21 "Organized Crime and Terrorism Act of 2016"; Penal Code, Art. 434-15-2.

22 "Intelligence Act of 2015."

23 Internal Security Code, Art. L871-1, L881-2..

24 Ibid., Art. L871-1.

25 For a more comprehensive review of France's legal framework for hacking, see European Parliament Directorate-General for Internal Policies, "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices," March 2017, 72-76, available at http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

26 LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (1) [Law 2011-267 of March 14, 2011, Guidance and Programming for the Performance of Internal Security], available at https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&categorieLien=id].

*This sentence was revised on August 9, 2017 to clarify the law's provisions.

27 Brian Harley, "French Security Bill to Authorize Internet Filtering," *The Columbia Science and Technology Review*, March 1, 2010, http://stlr.org/2010/03/01/french-security-bill-to-authorize-internet-filtering/; Emilien Ercolani, "Loppsi : Qui Pourra Installer les Mouchards Informatiques?" *L'informaticien*, November 7 2011, http://bit.ly/1MBpDkh.

28 Criminal Procedure Code, Arts. 706-102-1, 706-102-2.

29 Ibid., Arts. 706-102-4 et. seq.

30 "Intelligence Act of 2015."

31 Internal Security Code, Art. L821-2.

32 Felix Treguer, "Internet Surveillance in France's Intelligence Act," *HAL*, November 19, 2016, https://halshs.archives-ouvertes.fr/halshs-01399548/document.

33 Internal Security Code, Art. L821-8.

34 Eugene Kaspersky, "Animals in the APT Farm," *Securelist* (a Kaspersky blog), March 6, 2015, https://securelist.com/blog/research/69114/animals-in-the-apt-farm/; Lorenzo Franceschi-Bicchierai, "Meet Babar, a New Malware Almost Certainly Created by France," *Motherboard*, February 18, 2015, https://motherboard.vice.com/en_us/article/meet-babar-a-new-malware-almost-certainly-created-by-france; Lorenzo Franceschi-Bicchierai, "Meet Casper: Yet Another Malware Likely Created by France for Surveillance," *Motherboard*, March 5, 2015, https://motherboard.vice.com/en_us/article/meet-casper-yet-another-malware-likely-created-by-france-for-surveillance.

35 Patryk Pawlak and Gergana Petkova, "State-Sponsored Hackers: Hybrid Armies?," Brief, Alert (Paris: European Union Institute for Security Studies (EUISS), January 30, 2015), 2, http://www.iss.europa.eu/publications/detail/article/state-sponsored-hackers-hybrid-armies/; European Parliament Directorate-General for Internal Policies, "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices," March 2017, 60, available at http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

36 European Parliament Directorate-General for Internal Policies, "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices," March 2017, 72-76, available at http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

37 Bhairav Acharya, Kevin Bankston, Ross Schulman and Andi Wilson, "Deciphering the European Encryption Debate: Germany," New America's Open Technology Institute, July 2017, available at https://www.newamerica.org/oti/blog/deciphering-european-encryption-debate-germany/.

38 "Organized Crime and Terrorism Act of 2016"; Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique [Law 2016-1321 of October 7, 2016 for a Digital Republic], for the purposes of this paper, this will be called the "Digital Republic Act of 2016," available at https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id; Amendment n° CL92 to National Assembly bill 3318 (January 4, 2016) Nathalie Kosciusko-Morizet, et.al., available at http://www.assemblee-nationale.fr/14/amendements/3318/CION_LOIS/CL92.asp; Amendment n° 90(Rect) to National Assembly bill 3515 (February 23, 2016) Phillip Goujon, et.al.,

available at http://www.assemblee-nationale.fr/14/amendements/3515/AN/90.asp; Amendment nº 221 to National Assembly bill 3515 (February 25, 2016) Eric Ciotti, et.al., available at http://www.assemblee-nationale.fr/14/amendements/3515/AN/221.asp. Amendment nº 532 to National Assembly Bill 3515 (February 29, 2016) Yann Galut et. al., available at http://www.assemblee-nationale.fr/14/amendements/3515/AN/532.asp; Amendment No. 533 to National Assembly Bill 3515 (February 29, 2016) Yann Galut et. al., available at http://www.assemblee-nationale.fr/14/amendements/3515/AN/533.asp; Senate Amendment nº 445 (February 29, 2016) Michel Mercier, available at http://www.senat.fr/amendements/commissions/2015-2016/445/Amdt_COM-80.html.

39 Amendment nº 90(Rect) to National Assembly bill 3515.

40 Criminal Procedure Code, Art. 60-1; Penal Code, Art. 434-15-2.

41 Amendment nº CL92 to National Assembly bill 3318; Amendment nº 221 to National Assembly bill 3515.

42 Loi nº 2016-1321 du 7 octobre 2016 pour une République numérique [Law 2016-1321 of October 7, 2016 for a Digital Republic].

43 Amendment nº CL92 to National Assembly bill 3318.

44 Transcript of Proceedings of the National Assembly (January 13, 2016): http://www.assemblee-nationale.fr/14/cr-cloi/15-16/c1516035.asp.

45 Amendment nº CL92 to National Assembly bill 3318.

46 Transcript of Proceedings of the National Assembly (January 13, 2016).

47 Ibid.

48 James Comey "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" [remarks, Brookings Institution, Washington, D.C., October 16, 2014] available at https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

49 Glynn Moody, "French Government Rejects Crypto Backdoors As "the Wrong Solution"," *Ars Technica*, January 14, 2016, https://arstechnica.co.uk/tech-policy/2016/01/french-government-rejects-crypto-backdoors-as-the-wrong-solution/; Guillaume Champeau, "Chiffrement : Le Gouvernement Rejette Les Backdoors," *Numerama*, January 13, 2016, http://www.numerama.com/politique/138689-chiffrement-le-gouvernement-rejette-les-backdoors.html.

50 Guillaume Champeau, "Chiffrement : Le Gouvernement Rejette Les Backdoors," *Numerama*, January 13, 2016, http://www.numerama.com/politique/138689-chiffrement-le-gouvernement-rejette-les-backdoors.html.

51 Transcript of Proceedings of the National Assembly (January 13, 2016); Zack Whittaker, "NSA Suspected in Juniper Firewall Backdoor Mystery, but Questions Remain," *ZDNet*, December 23, 2015, http://www.zdnet.com/article/nsa-suspected-in-juniper-firewall-backdoor-mystery-but-questions-remain/.

52 Transcript of Proceedings of the National Assembly (January 13, 2016).

53 Ibid.

54 Ibid.

55 Daniel Severson, "The World's Not Waiting for California: France Moves to Enforce Decryption," *Lawfare*, March 7, 2016, https://www.lawfareblog.com/worlds-not-waiting-california-france-moves-enforce-decryption.

56 Bill nº 3473 in the National Assembly, http://www.assemblee-nationale.fr/14/projets/pl3473.asp.

57 See generally "Current Legal Landscape," 4.

58 Amendment nº 90(Rect) to National Assembly bill 3515.

59 Amendment nº 90(Rect) to National Assembly bill 3515.

60 Ibid.; Patrick Howell O'Neill, "French Bill Carries 5-year Jail Sentence for Company Refusals to Decrypt Data for Police," *Daily Dot*, March 3, 2016, https://www.dailydot.com/layer8/france-encryption-decryption-law-punish/.

61 Transcript of Proceedings of the National Assembly (March 3, 2016), http://www.assemblee-nationale.fr/14/cri/2015-2016/20160141.asp.

62 Helene Fouquet and Marie Mawad, "French Legislation Would Force Apple to Unlock Data," *Boston Globe*, March 8, 2016, https://www.bostonglobe.

com/business/2016/03/08/france-clears-bill-that-could-force-apple-unlock-terror-data/obHccWlCH8ZFpbjvPmXJ9J/story.html.

63 Transcript of Proceedings of the National Assembly (March 3, 2016), http://www.assemblee-nationale.fr/14/cri/2015-2016/20160141.asp.

64 Ibid.

65 Senate Amendment n° 445e (February 29, 2016) Michel Mercier, available at http://www.senat.fr/amendements/commissions/2015-2016/445/Amdt_COM-80.html.

66 Report n° 491 of the Committee of Laws of the Senate (March 23, 2016): http://www.senat.fr/rap/l15-491-1/l15-491-11.pdf.

67 Ibid.

68 Amendment n° 532 to National Assembly Bill 3515; Amendment n° 533 to National Assembly Bill 3515.

69 Ibid.

70 Ibid.

71 Transcript of Proceedings of the National Assembly (March 3, 2016).

72 Cyrus R. Vance Jr., François Molins, Adrian Leppard and Javier Zaragoza, "When Phone Encryption Blocks Justice," *New York Times*, August 12, 2015, https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html.

73 Transcript of Proceedings of the National Assembly (March 3, 2016).

74 Ibid.

75 Ibid.

76 Ibid.

77 Ibid.

78 Ibid.

79 Ibid.

80 Ibid.

81 Ibid.

82 Amendment n° 221 to National Assembly Bill 3515.

83 Daniel Severson, "The Encryption Debate in Europe," Aegis Paper Series No. 1702, The Hoover Institution (March 2017): http://www.hoover.org/sites/default/files/research/docs/severson_webreadypdf.pdf.

84 Transcript of Proceedings of the National Assembly (March 3, 2016).

85 Ibid.

86 Ibid.

87 Ibid.

88 Ibid.

89 Ibid.

90 Daniel Severson, "The World's Not Waiting for California: France Moves to Enforce Decryption," *Lawfare*, March 7, 2016, https://www.lawfareblog.com/worlds-not-waiting-california-france-moves-enforce-decryption.

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

92 Letter from the Interior Ministers of France and Germany to the European Commission, February 12, 2017, available at https://regmedia.co.uk/2017/02/28/french_german_eu_letter.pdf; Iain Thomson, "Germany, France Lobby Hard for Terror Busting Encryption Backdoors – Europe Seems to Agree," *The Register*, February 28, 2017, https://www.theregister.co.uk/2017/02/28/german_french_ministers_breaking_encryption/.

93 Emmanuel Macron, "Les Acteurs de l'Internet, S'ils Persistent Dans Leur Position, Devront Assumer Un Jour D'avoir Été Complices D'attentats. #LutteTerrorismepic.twitter.com/otqG8LNIMR," microblog, @EmmanuelMacron, (April 10, 2017), https://twitter.com/EmmanuelMacron/status/851380639261765632.

94 Sébastian Seibt, "French Candidate Macron Targets Encryption in Fight Against Terrorism," *France 24*, April 13, 2017, http://www.france24.com/en/20170412-candidate-macron-encryption-fight-terror-whatsapp-telegram.

95 Bhairav Acharya, Kevin Bankston, Ross Schulman and Andi Wilson, "Deciphering the European Encryption

Debate: United Kingdom," New America's Open Technology Institute, June 2017, available at https://www.newamerica.org/oti/policy-papers/deciphering-european-encryption-debate-united-kingdom/.

96 Natasha Lomas, "European MEPs Want to Ban States from Backdooring Encryption," *TechCrunch*, June 20, 2017, https://techcrunch.com/2017/06/20/european-meps-want-to-ban-states-from-backdooring-encryption/.

97 "Texte Du Plan d'Action Franco-Britannique Pour Lutter Contre L'utilisation de L'internet à des Fins Terroristes," Ministère de l'Interieur, June 14, 2017, https://www.interieur.gouv.fr/Actualites/Communiques/Utilisation-de-l-Internet-a-des-fins-terroristes-plan-d-actions-franco-britannique.

98 Ibid.

99 Ibid.

100 "Digital Republic Act of 2016."

101 "What Is the CNIL's Position in Terms of Encryption?" CNIL, July 18, 2017, https://www.cnil.fr/en/what-cnils-position-terms-encryption.

102 Ibid.

103 Martin Untersinger, "La CNIL Très Favorable au Chiffrement des Données," *Le Monde*, April 9, 2017, http://www.lemonde.fr/pixels/article/2016/04/09/la-cnil-tres-favorable-au-chiffrement-des-donnees_4899172_4408996.html#hWGj18UR5tA1CCWt.99.

104 European Parliament Committee on Civil Liberties, Justice and Home Affairs, Draft Report on Encryption, June 9, 2017, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-606.011%2B01%2BDOC%2BPDF%2BV0%2F%2FEN; Natasha Lomas, "European MEPs Want to Ban States from Backdooring Encryption," *TechCrunch*, June 20, 2017, https://techcrunch.com/2017/06/20/european-meps-want-to-ban-states-from-backdooring-encryption/.

This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of New America content when proper attribution is provided. This means you are free to share and adapt New America's work, or include our content in derivative works, under the following conditions:

- **Attribution.** You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit **creativecommons.org**.

If you have any questions about citing or reusing New America content, please visit **www.newamerica.org**.

All photos in this report are supplied by, and licensed to, **shutterstock.com** unless otherwise stated. Photos from federal government sources are used under section 105 of the Copyright Act.