
BHAIRAV ACHARYA, KEVIN BANKSTON, ROSS SCHULMAN, ANDI WILSON

# DECIPHERING THE EUROPEAN ENCRYPTION DEBATE: UNITED KINGDOM

JUNE 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.

## Acknowledgments

The authors would like to thank Amie Stepanovich, Scarlet Kim, Javier Ruiz, and our other external reviewers for their input and comments on this paper. This paper does not necessarily reflect their views. We also 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 **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 first of those papers, focused on the encryption debate in the United Kingdom. The other papers in the series cover the encryption debates in Germany and France.

## Contents

# INTRODUCTION

The United Kingdom is no stranger to policy debates over encryption. Since the early 2000s, U.K. lawmakers have debated encryption's privacy and cybersecurity benefits, as well as the obstacles it can create for law enforcement and intelligence investigators. The recent increase in the availability of default device encryption and end-to-end messaging services (messaging apps where only the users have the keys to decrypt their messages) has led to growing concern by law enforcement and intelligence investigators about how best to address situations where only the subjects of investigations themselves may possess the keys to their encrypted data. These concerns have prompted renewed debate and lawmaking in the U.K. around encryption.

January 2015 saw the escalation of the encryption fight in a number of nations around the world, including the U.K. Not long after the introduction of default iPhone encryption in the U.S., and just days after the Charlie Hebdo shooting in Paris had renewed fears of terrorism across Europe, Prime Minister David Cameron spoke out. His comments suggested that there should be no "means of communication" which "we cannot read," and were widely interpreted to suggest a legal ban on end-to-end encrypted messaging apps.[6] These remarks sparked concern that the U.K. government was mounting an anti-encryption policy push.[7] That same week, Cameron reportedly pressed the issue in a visit with U.S. President Barack Obama, demanding greater cooperation from Silicon Valley companies to support the U.K.'s anti-terrorism efforts.[8]

In this climate of increased attention to encrypted communications, the bill that would eventually become the Investigatory Powers Act (IPA) was introduced in Parliament in late 2015. The Investigatory Powers Bill (as it was called before it was passed into law) sought to authorize sweeping new surveillance powers while forcing internet service providers (ISPs) to retain their customers' records for 12 months. Nicknamed the "Snoopers' Charter" by the press and civil society, the bill also explicitly authorized both targeted and mass computer hacking that a variety of British intelligence and law enforcement agencies had already been secretly engaging in for years. Most relevant to the current debate on encryption, it authorized cabinet ministers to issue secret orders to a broadly-defined set of communications service providers (CSPs) requiring that they create and maintain the capability to assist with lawful surveillance, including having the capability to decrypt their users' encrypted communications. The final version of the bill passed in November 2016 despite strong criticism from some of the world's biggest tech companies,[9] a large number of civil society organizations,[10] and three United Nations special rapporteurs.[11]

The IPA came into force on December 30, 2016, but confusion over this law remains, primarily because it is still unclear whether, when, or how the government may use the IPA to compel providers to redesign their encrypted services to facilitate government access. Meanwhile, new domestic terrorist incidents, such as the March 2017 attack outside of the Houses of Parliament, prompted renewed statements against encryption from Home Secretary Amber Rudd, even before it was known if encryption played a role in the attacks.[12] Theresa May, who was the IPA's primary champion when she served as Home Secretary, is now Prime Minister, and her party's manifesto for the recent election vowed to end safe spaces for terrorists online, which some have interpreted as referring to the use of encryption.[13] Suffice to say, end-to-end messaging services and device encryption tools are likely to face resistance from government officials in the U.K. for the foreseeable future.

This paper aims to summarize the state of the encryption debate in the U.K., in order to enable comparison with similar debates in the U.S., Germany, and France, and to see what lessons from the British experience might be applied by advocates and policymakers that continue to defend encryption both in the U.K. and elsewhere. First, the paper will examine the U.K. laws and regulations in force today that impact encryption, trying to gauge the extent to which they may require the re-engineering of products to include backdoors or be used to prohibit encrypted products without backdoors (what we'll collectively call "undermining encryption").

The paper will then provide additional political background on the state of the debate, describing how it got to the point where it is now, identifying the parties to the debate and their arguments, and making predictions about the future of the U.K. encryption debate. It will end with strategic recommendations for advocates of encryption about how to address threats to encryption and how pro-encryption groups can be more effective.

> **Since the early 2000s, U.K. lawmakers have debated encryption's privacy and cybersecurity benefits, as well as the obstacles it can create for law enforcement and intelligence investigators.**

# THE CURRENT LEGAL LANDSCAPE: UNDERSTANDING THE INVESTIGATORY POWERS ACT

The recently-enacted IPA, among other things, authorizes the U.K. government to set technical requirements regarding communications operators' ability to provide user information upon request, which may include requiring them to maintain the ability to decrypt it. It also authorizes the government to engage in legally sanctioned investigative hacking, and codifies its broader set of communications surveillance authorities. The law went into effect at the end of 2016, so there is still little information publicly available about how it will be used or what exactly the government believes it permits. What we do know is that, broadly speaking, the law grants the U.K. government the power to compel a variety of private parties to perform a poorly-defined scope of actions related to encryption and other digital security measures. The government concluded a public consultation on a set of "Codes of Practice" for the law in April 2017. Codes of Practice are common legislative tools in the U.K., used to clarify law and provide a safe harbor for those who follow them, though they do not carry the force of law.[14] These codes could give additional insight into application of the law, but results from the consultation process have not yet been published.

The pertinent pieces of the law to the encryption debate regulate what are termed "telecommunications operators" (confusingly, in the accompanying Codes of Practice, these entities are referred to as "communication service providers"). Any company that electronically transfers messages from one person to another could be covered under this law as an operator, including Microsoft (Skype), Google (Gmail), Apple (iMessage), and many others. Two sections of the law in particular, sections 253 and 252, impose obligations on operators that may require them to undermine the encryption used by their customers. In addition, a set of sections starting with section 99 lays out the government's ability to issue "equipment interference" warrants (i.e., warrants for targeted remote hacking into specific devices for intelligence or law enforcement purposes, though the list of devices can be a large one) while sections 176 through 198 authorize large-scale hacking of devices (such as all of the mobile phones in a geographic area)[15], offering

another potential avenue for accessing encrypted communications. We'll begin by reviewing the provisions related to technical assistance by communications providers, then briefly discuss the new hacking authorities.

## Technical Capability Notices Under the IPA: Can They Demand Backdoors into Encryption?

There are several sections of the IPA that require cooperation from telecommunications service providers and technology companies. Section 253 of the IPA authorizes the government to serve operators with "technical capability notices."[16] These notices can be used to demand technical modifications to the operator's product to facilitate surveillance, and compel operators to maintain those capabilities to address future surveillance demands that the government may make.[17] The section is very broadly drafted, and could be read to cover virtually any surveillance activity or new technology. With such open-ended provisions, the manner in which the law is interpreted will be critical in understanding how the government engages with operators.

Notices under section 253 may be issued if a Secretary of State (in particular, one of three specific cabinet ministers)[18] determines that it is necessary "for securing that the operator has the capability to provide any assistance which the operator may be required to provide."[19] That "capability" includes the ability of the operator to comply with any surveillance, bulk or individualized, ordered under the IPA.

There are a number of steps that the Secretary must take when issuing a technical capability notice. First, he or she must consult with the entity that will be the recipient of the notice.[20] Second, he or she must take into account a number of considerations, including technical feasibility of compliance, the number of users likely affected, and the likely cost of compliance.[21] If the notice being issued will compel the "removal… of electronic protection," he or she must also at this point take into account the "technical feasibility and cost" of the notice.[22] After weighing those considerations, the Secretary must thirdly decide that the technical capability being demanded is both necessary for guaranteeing access to some information pursuant to a warrant in the future, and proportionate to "what is sought to be achieved" by the notice.[23] Finally, the issuing of the notice must be approved by a Judicial Commissioner. The Judicial Commissioner's review is focused on whether the Secretary followed the procedures laid out in the law.[24]

The types of obligations that can be contained in a technical capability notice are to be specified by a cabinet minister through regulations that have not yet been promulgated, and as per the statute can explicitly include "the removal of electronic protection applied by or on behalf of the operator."[25] This clause is broadly understood to include the decryption of encrypted material, but for a variety of reasons discussed below, it is not yet clear whether a notice requiring the "removal of electronic protection" could be used to require (e.g.) an end-to-end messaging service provider to redesign its system so that the provider could decrypt the users' messages. As also discussed below, a leaked version of the draft regulations offers no new clarity on this score.

Considering the breadth and vagueness of the IPA's language, how the IPA will be used by the government to compel operators to comply with these technical notices remains an open question. During debates on the bill, civil society groups argued that it contained provisions "that could be used to undermine encryption"[26] or "[force] companies [to] compromise their software to make the encryption less effective."[27] Similar criticisms were leveled by technology companies, saying that early drafts of the IPA could require backdoors in their products, harming their customers and weakening cybersecurity.[28]

The government's responses during the legislative process were varied and contradictory. In January 2015, Prime Minister Cameron said publicly that tech companies should not enable communications

that "we [the government] cannot read."[29] Cameron echoed that opinion in Parliament in June when he said that he wanted the government to be able to have access to all electronic communications with a warrant.[30] Although ensuring such access would necessarily entail the elimination or backdooring of end-to-end encryption, Cameron's representatives confusingly indicated that they wanted no such thing. For example, when Cameron's minister for internet safety and security Baroness Joanna Shields was asked in the House of Lord's whether she could "absolutely confirm that there is no intention in forthcoming legislation either to weaken encryption or provide back doors," Shields replied: "I can confirm that there is no intention to do that; that is correct." She continued, somewhat confusingly, to say that "The Prime Minister did not advocate banning encryption; he expressed concern that many companies are building end-to-end encrypted applications and services and not retaining the keys." Considering the Prime Minister's apparent intent that the IPA would address his concern, such comments don't offer much clarity about the law's meaning, perhaps intentionally so. Notably, even assuming the IPA can be used to require providers served with a capability notice to backdoor their encrypted products, that would not be equivalent to a general "ban" on that encryption.[31] Such apparent word-games echo the confusingly contradictory rhetoric of former FBI Director James Comey, who has repeatedly stated that he "loves strong encryption," and isn't proposing "backdoors," but simply wants to ensure that providers can always hand over users' content in response to a lawful order (which would necessarily require backdoors and/or a ban on end-to-end encryption).[32]

Another example of confusing and contradictory government statements about encryption and the IPA was a fact sheet issued by the government which recognised the economic and privacy benefits of encryption and claimed that the IPA did not mandate the installation of backdoors. This would seem to be a clear indicator of the government's position—yet the government later removed the fact sheet from its website without explanation as to whether this indicated an official change of policy or messaging.[33] The parliamentary joint committee[34] on the IPA, hoping to dispel any further uncertainty, recommended that the government "make explicit on the face of the bill that operators 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."[35] The joint committee's recommendation was not heeded, however, and the IPA as passed bluntly mandates that operators fulfill their obligations to "remov[e] electronic protection" without any explicit carve-out for encrypted messaging services.[36]

To address criticism surrounding its encryption provisions and to reconcile the conflicting statements on the bill from government officials, the bill was amended in March 2016.[37] The revisions, which eventually ended up in the Interception of Communications Code of Practice (the proposed Code of Practice for section 253) rather than the text of the law itself, clarified that companies would only be forced to remove encryption that the "company has itself applied to communications or data, or where those protections have been applied on behalf of that communications service provider, and not to encryption applied by any other party" and where practical do so.[38] Even with these clarifications, however, there are still questions about whether an end-to-end encrypted messaging service meets this requirement. As one commentator put it, "the bill does make it quite clear that a CSP can only be required to remove encryption that it has itself applied, or has been applied on its behalf. But if the software on my device encrypts my data, is it working on my behalf or on behalf of the software vendor and service provider [or not]? Both interpretations are defensible."[39]

Since many questions about how to interpret these vague provisions still remain, several Codes of Practice will be released to support the IPA, and are intended to explain how the statute's various surveillance powers can be exercised.[40] Five of these Codes of Practice went through a public comment period in early 2017 (though they have

not been finalized at the time of publication) and are meant to serve as explanations for ambiguous or undefined terms in the law.[41] The Interception of Communications Code of Practice reiterates that obligations under the technical capability notices could include the "removal of electronic protections," but offers little new clarity on the end-to-end question.[42]

> **The full scope of what a technical capability notice under Section 253 or a national security notice under Section 252 can demand of a communications provider is unclear, and contested.**

Although offering no new guidance on how technical capability notices will apply to providers of encrypted services, a troublesome provision in Paragraph 8.32 of the Equipment Interference Draft Code of Practice may have serious implications for such providers. This Code of Practice—on government hacking—demands that "communications services providers which have been given a technical capability notice must notify the [cabinet minister] of…new services and relevant products in advance of their launch."[43] This power has the potential to give the U.K. government the ability to influence product design decisions by demanding surveillance capabilities before the design process has progressed far enough to make changing the product or undermining its encryption technically infeasible and thus outside the scope of the law. In other words, if exploited aggressively, the IPA may be used to enforce a de facto ban on future end-to-end encrypted products.

However, the technical capability notices authorized in section 253 of the IPA aren't the only IPA notices that might impact encrypted services. Section 252 of the IPA allows a Secretary of State to serve operators with "national security notices," an even broader authority which could also be used to undermine encryption. These notices obligate the recipient to take actions identified by the minister that he or she deems are "necessary for national security" and "proportional to what is sought to be achieved."[44] A national security notice can compel the recipient to "carry out any conduct" to "facilitate anything done by an intelligence service" or to respond to an emergency. As with the technical capability notices, this section is written so broadly that it potentially encompasses the removal or undermining of a system of encryption. The national security notices are only constrained by a requirement that they are not used to achieve a result the "main purpose of which" would otherwise require a warrant or authorization under the law.[45] The strength of this limitation, however, will turn on the interpretation of "main purpose," which is not defined in the IPA. In addition, some in civil society have expressed the concern that if the national security notice is aimed at subverting encryption for a future investigation (which would require a warrant in the future but not in the present), it might also not fall under this limitation. The Codes of Practice for section 252 are of little help in illuminating the boundaries of the notices, other than to acknowledge that "[i]t is not possible to give a list of the full range of the steps that telecommunications operators may be required to take in the interests of national security."[46]

As is obvious from the above, the full scope of what a technical capability notice under Section 253 or a national security notice under Section 252 can demand of a communications provider is unclear, and contested. To make matters worse, the IPA makes it impossible to have an informed public debate on the issue, because the exercise of both authorities will take place in complete secrecy: communications services providers under the law "must not disclose the existence or contents of the notice to any other person without the permission of the Secretary of State."[47] Petitioning the Secretary of State directly is the only means of lifting these gag orders and the law does not specify the process by which such a decision is made.[48] Similar secrecy surrounds the exercise of another key set of authorities under the IPA: the government's authority to conduct hacking operations.

## The State of Government Hacking in the U.K.

Many governments, including the U.K., have begun remotely hacking into communications devices and networks to obtain data, both encrypted and unencrypted, sought by their intelligence and law enforcement agencies. Sections 99 through 135 of the IPA codify the power of the government to gain access to any "equipment" (which can include a laptop or mobile phone) by "interfering" with the equipment (i.e., hacking into it).[49] "Equipment" is defined in the IPA as any thing producing electromagnetic or acoustic emissions, which effectively includes every possible piece of computing equipment. "Interference" is not precisely defined in the IPA. While this section has elements that distinguish it from the "bulk" warrants described below, even these warrants permit a variety of equipment to be targeted at once, such as many different devices in multiple places, if they are all of interest in a single investigation.

The law provides for a variety of processes for issuing equipment interference warrants, depending on the type of target and the type of investigation being conducted. For example, a Secretary of State is responsible for issuing warrants for intelligence services,[50] the Scottish Ministers for equipment located only in Scotland,[51] and "a law enforcement chief" for criminal issues.[52] In all instances, the issuing authority must determine that the conduct being authorized under the warrant is both necessary and proportionate to the result being sought. For criminal matters, equipment interference warrants are limited to cases where that interference is necessary to prevent or detect "serious crime,"[53] while in intelligence cases it must be necessary to the interests of national security or the economic well-being of the United Kingdom.[54]

In addition to the requirements of necessity and proportionality, the issuing authority must also ascertain that procedures are in place to control the retention and disclosure of any information gathered via the hacking.[55] The Draft Code of Practice related to equipment interference further explains that the possibility of collateral intrusion of the privacy of non-targets must be considered and plans to minimize such information are integral to the proportionality of a warrant.[56] Finally, in all cases above the Judicial Commissioners must approve the issuance of the warrant except in urgent circumstances when the warrant may issue immediately but must be reviewed within three working days.[57] As with the Technical Capability and National Security notices, the remit of the Judicial Commissioners is restricted to whether the proper procedures have been applied.

> **The breadth of these authorities and the secrecy under which they operate highlight the need for extensive and rigorous independent oversight as well as a clear and robust ability for providers to challenge them in court.**

While the above hacking authorities are worrisomely broad, they are at least meant to be used against particular targets, and those targets must be tied in some way to an investigation. By contrast, Sections 176 through 198—authorizing hacking in bulk in foreign intelligence cases—contain no such restrictions. These sections authorize equipment interference in the case of large numbers of devices (for which the government obtains a "bulk warrant") as long as the purpose of the warrant is to gather "overseas-related" communications or information.[58] The government released two "case studies" for when a bulk equipment interference warrant would be used, and in both cases the "target" was the entirety of a designated geographic area.[59]

As with the technical capability and national security notices described previously, any companies compelled to provide assistance with either targeted device interference or untargeted

bulk hacking are forbidden from speaking about their experience. Both the breadth of these authorities and the secrecy under which they operate highlight the need for extensive and rigorous independent oversight as well as a clear and robust ability for providers to challenge them in court. Unfortunately, the law fails to hit that mark.[60]

## Oversight Over Technical Capability and National Security Notices and Government Hacking

The secrecy around the various IPA notices and warrants, combined with the uncertainty surrounding the U.K.'s power to compel backdoors through these authorities, means that the boundaries of what is permitted will inevitably be fought over by the government and the companies receiving notices, as well as the oversight bodies created by other provisions of the law, such as the Investigatory Powers Commissioner (IPC). That Commissioner will be an individual appointed by the Prime Minister, who will be supported by a number of Judicial Commissioners, also appointed by the Prime Minister, who will report to the Commissioner. Certain warrants and notices issued under the IPA require the approval of a Judicial Commissioner, including technical capability and national security notices, based on review of the issuing Secretary of State's conclusion that the notice in question is "necessary and proportionate."[61] Hacking warrants are similarly subject to the same so-called "double-lock" authorization safeguard.[62] This process provides some new protection for privacy and human rights and is a small step forward for the U.K., where only the approval of the Home Secretary has been necessary to carry out a traditional wiretap. However, there is concern that rather than reviewing the actual substance of the authorizing Secretary of State's judgment regarding necessity and proportionality or weighing the evidence that supports it, the commissioners will simply be ensuring that the Secretary's decision-making was procedurally adequate.[63]

The IPA also calls for a Technical Advisory Board (TAB), to be made up of people representing the interests of operators that may receive notices and those that apply for warrants or authorizations, as well as anyone else that the Secretary of State thinks ought to be present. The TAB must be consulted by the Secretary of State before regulations on the issuance of technical capability notices are issued, though its responses are advisory only.[64]

In addition to review prior to the issuance of notices, the recipient of a technical capability notice under the IPA can refer the notice back to the Secretary of State for review. The Secretary must then consult with the TAB and a Judicial Commissioner as part of its review: the TAB "must consider the technical requirements and the financial consequences" for the notice recipient, and the commissioner must consider whether the notice is proportionate.[65] If the notice is upheld after review, the provider may appeal to the U.K.'s Investigatory Powers Tribunal, an independent appeals court for dealing with surveillance matters that was created by the Regulation of Investigatory Powers Act 2000.[66] The Tribunal can hear evidence in either an open or closed session and has procedures for dealing with classified materials. From there, the IPA generally provides a means to appeal (only) questions of law to the U.K.'s regular appellate courts.[67] However, some in civil society have raised the concern that the gag orders that accompany assistance demands may prevent companies from petitioning the regular courts, or international courts. Assuming that secrecy requirements do not prevent it, companies that choose to fight a notice could potentially bring a challenge in the European Court of Human Rights or the Court of Justice of the European Union, which are discussed in more detail below.

It remains to be seen how effective any of these routes to appeal may eventually be, but some speculate that the U.K. government may be hesitant to aggressively use technical capability notices against end-to-end encryption providers for fear of losing a legal fight with the provider, whether as part of a Secretary of State's review or otherwise.[68] For this reason and more, the details of the IPA's ultimate implementation are still hard foresee—but looking to the past might help us better predict the future, and assess how to go forward from here.

# HOW DID WE GET HERE, AND WHERE ARE WE GOING?

## U.K.'s First Crypto Debate: Mandatory Key Disclosure in the Regulation of Investigatory Powers Act 2000

Although countries like the U.S. have had public conversations on whether to regulate or restrict encryption as far back as the early 1990s,[69] the first anti-encryption provisions of British surveillance law were not introduced until 2000, under the Regulation of Investigatory Powers Act (RIPA).[70] RIPA, the government said, would bring the U.K.'s surveillance activities in-line with the European Union's view of the European Convention on Human Rights.[71] The legislation governed the use of covert surveillance powers, including the interception of communications, directed surveillance, acquisition of communications metadata, and the ability to access encrypted content. Specifically, RIPA allowed the government to order both companies and individuals to surrender their encryption keys to law enforcement if the government could prove that access to the encrypted data was in the interests of national security, to prevent or detect crime, or for the U.K.'s economic well-being.[72] RIPA introduced criminal penalties for refusing to obey a key disclosure order and for not keeping such an order secret. Failure to comply could mean a prison sentence of up to two years for cases not involving national security or five years for cases that do.[73]

RIPA's key disclosure provisions were highly controversial from the start. The British government claimed that these powers were necessary to fight terrorism, but lawmakers received a huge amount of criticism from human rights organizations concerned about its impact on privacy.[74] Dogged by privacy and implementation concerns, these provisions did not come into force until 2007[75]—and were quickly applied in a wide range of criminal cases having nothing to do with terrorism, drawing even more criticism from privacy advocates.[76] Indeed, according to information released in annual reports from the Chief Surveillance Commissioner, it wasn't until 2013 that a key disclosure order was issued in a terrorism investigation.[77] By that time, however, more and more messages were beginning to be end-to-end encrypted in cases where the authorities didn't want to tip off the investigation by demanding keys from those suspects, but couldn't demand keys from the providers because the providers didn't have them. This tension was just one of the conditions that set the stage for a debate

about new legislation to broadly expand the U.K. government's surveillance authorities, including its authority to demand technical assistance from providers.

## The Fight Over IPA: Key Players and Arguments

Edward Snowden—no stranger to the world's most powerful surveillance capabilities—described the new IPA as having legalized "the most extreme surveillance in the history of western democracy."[78] Especially considering its explicit authorization of bulk surveillance and bulk hacking, he's probably not too far off the mark. Predictably, then, the IPA was the subject of significant debate between a wide range of stakeholders, although very few members of Parliament were ultimately willing to vote against it. In March 2016, the Investigatory Powers Bill passed its first substantive vote and debate in the House of Commons. Of the 650 members of the House, a total of 266 voted for the Investigatory Powers Bill and just 15 voted against. Despite having criticized the bill for the broad scope of surveillance it authorized and its lack of privacy protections,

> **Civil society organizations, both domestically and internationally, were universally critical of the expanded surveillance powers and potential for dangerous encryption restrictions.**

the Labour Party abstained from the vote for fear of sinking the bill entirely—and, presumably, for fear of looking weak on terrorism compared to their Conservative counterparts.[79] Shadow Home Secretary Andy Burnham said that killing the bill "would be to abdicate our responsibility to the police, security services, and, most importantly, the public," while leaving British citizens with the much weaker privacy safeguards provided under the Data Retention and Investigatory Powers Act 2014 (an interim bill rushed into law when the European Court of Justice overturned parts of the original RIPA).[80] The Scottish National Party also abstained, after expressing "grave concerns" about the bill.[81] Their spokesperson said that "the powers to retain internet connection records and the bulk powers go beyond what is currently authorised in other western democracies and thus could set a dangerous precedent and a bad example internationally."[82] The Liberal Democratic Party voted against the bill, stating that "the bill still has no section on privacy, no meaningful independent judicial oversight, and no clarity on whether British businesses, just like Apple in the U.S., would be forced to break the encryption they use to protect their customers."[83] However, the Conservative Party, which held the majority of seats in the House of Commons at the time of the vote, was in strong support—party leader and then-Home Secretary Theresa May was in fact the primary architect of the IPA[84]—such that a bill that was widely criticized by a broad swath of the House of Commons nevertheless easily passed by a wide margin.[85]

Civil society organizations, both domestically and internationally, were universally critical of the expanded surveillance powers and potential for dangerous encryption restrictions. Domestic organizations, including the Don't Spy On Us coalition, submitted comments alongside briefings, petitions, advocacy campaigns,[86] and even a legal challenge brought by some of their members.[87] Article 19, a British human rights organization that works to preserve freedom of expression, argued that "regulations requiring operators either to remove encryption services upon request, or to reduce the effectiveness of encryption… would fundamentally undermine the use of end-to-end encryption and therefore the security of our online communications and transactions."[88] Liberty, another of the U.K.'s leading privacy and civil liberties organizations, succinctly stated that "undermining encryption seriously jeopardises the security of technologies, their users, and modern digital society as a whole."[89]

Organizations from outside the U.K. got involved, too. A coalition of international organizations,

including Access Now, the Electronic Frontier Foundation, and New America's Open Technology Institute (OTI),[90] submitted joint written evidence criticizing the bill's surveillance authorities as "exceedingly broad," noting that the technical capability provisions that might be used to undermine encryption "are particularly troubling and may make it harder for both large and small companies to protect their users."[91] OTI also submitted individual comments focused on the importance of encryption, and on the need to significantly narrow the bill's dangerously overbroad hacking authorities.[92] Three U.N. Special Rapporteurs also weighed in, specifically on the lack of oversight, and expressed concerns that the broad discretion to issue regulations that the bill provided "might lead to blanket restrictions on encryption that affect massive numbers of persons, which would most likely result in a breach of the requirements of necessity and proportionality."[93]

In addition to voicing concerns about the privacy impact of weakening encryption via the IPA, critics also focused on the economic impact. Civil society group Big Brother Watch warned the commission that by imposing a "requirement for companies to weaken or remove their encryption to comply with warrants, the U.K. could find itself a country which no technology company will want to engage with."[94] Similarly, the Center for Democracy and Technology suggested that forcing companies to weaken their encryption in order to comply with technical capability notices "would lead to a loss of confidence in U.K. technology companies globally and would damage investment in the broader U.K. technology sector."[95]

Especially considering the potential economic impact, companies and trade organizations from around the world also weighed in during the drafting process. The Reform Government Surveillance coalition, a group of U.S.-based internet and technology companies that works to strengthen the practices and laws regulating government surveillance,[96] expressed the need to establish a framework for lawful data requests while ensuring that citizens' human rights and privacy rights are protected.[97] The coalition was explicitly concerned about the draft requirements that companies be able to remove electronic protection on user communications or data.[98] Apple expressed concern that the bill was extending its power to overseas providers, as well as objecting to the mandatory decryption provisions.[99] They argued that the technical capability notice obligations would be exploited by bad actors abroad, that they lacked an adequate oversight mechanism, that the decryption duty would be too costly to comply with, and that it would impose a disproportionate burden on Apple's business.[100] Mozilla also filed a submission making similar arguments against obligations to weaken encryption.[101]

Concern about the IPA's impact on encryption wasn't limited to those outside of the government, either. The U.K.'s Information Commissioner, a government-appointed civil servant that reports to Parliament and serves as the U.K.'s data protection authority, argued that notices requiring the removal of electronic protection should not be permitted to lead to the removal or weakening of encryption. He noted that "obligations relating to the removal of electronic protection...could be a far

**In addition to voicing concerns about the privacy impact of weakening encryption via the IPA, critics also focused on the economic impact.**

reaching measure with detrimental consequences to the security of data and safeguards which are essential to the public's continued confidence in the handling and use of their personal information."[102] Meanwhile, the director of the U.K.'s Government Communications Headquarters (GCHQ — often considered the U.K.'s equivalent of the National Security Agency) expressed a similar sentiment at a public event, saying that "the solution is not, of course, that encryption should be weakened, let alone banned. But neither is it true that nothing can be done without weakening encryption. I am not in favour of banning encryption just to avoid doubt. Nor am I asking for mandatory backdoors."[103]

One part of the solution to the encryption "problem," at least from the government's point of view, is the new hacking authority provided by the IPA. For example, U.K. domestic law enforcement supported the expanded hacking provisions explicitly as a means to access encrypted information. In their joint submission to Parliament's Joint Committee on the Investigatory Powers Bill, the National Police Chiefs Council, HM Revenue and Customs, and the National Crime Agency declared: "[Hacking] already provides significant operational benefit to [law enforcement] by facilitating the obtaining of information and evidence that cannot be captured by other means—for example where encryption technology is being used to hide criminal communications."[104] The Home Office, too, alluded to the British government's intention of circumventing encryption by hacking: "Historically, the security and intelligence agencies have largely been able to find and follow their targets through the use of interception. This capability remains critical, but technological advances and the spread of ubiquitous encryption—wrapping information in an impenetrable blanket from sender to receiver—is resulting in an increasing number of circumstances where interception is simply not possible or effective," making hacking—in their view—a necessary alternative.[105]

While some in civil society see targeted government hacking as a preferable alternative to broadly demanding backdoors into encrypted products and services,[106] many civil society organizations still had concerns with the broad expansion of surveillance and hacking powers in the IPA, and especially the provisions for untargeted or "bulk" hacking. Human Rights Watch warned that, "[h]acking allows law enforcement to surreptitiously access data and communications directly from personal devices and other equipment, which can allow authorities to bypass encryption."[107] The Electronic Frontier Foundation highlighted that "equipment interference can give an attacker complete control of a communications device…granting access to all data and metadata on the device including, but not limited to, passwords for other systems, location data, cameras, and microphones, and allowing the attacker to execute arbitrary malicious code. It can be abused to plant incriminating evidence, deploy permanent malware, or rewrite existing data to any end."[108] And New America's Open Technology Institute, responding to the draft bill's clear statement that hacking was a means to bypass encryption, called for qualified prohibitions and strict regulation of hacking: "We believe that if [hacking] is to be used, it must be limited, and should only be authorized—if at all—in narrow circumstances with strong protections. Further, we believe that certain measures under consideration—specifically, use of [hacking] for bulk collection and adding new vulnerabilities in software updates—should be completely prohibited."[109]

The IPA ultimately passed despite such concerns, but the debate over that bill—and the government's often-confusing representations about what it did or did not intended the law to do—demonstrated that there is not a consensus, within or outside of government offices, on the best way to access encrypted data. Nor is there any clear understanding or agreement on how the IPA can or cannot be used to facilitate that access.

## What Does the Future Hold?

Unfortunately, no one has a crystal ball that allows us to see how this debate over encrypted information will evolve in the U.K. As of now, it is

probably safe to say that former-Home Secretary Theresa May's ascent to the role of Prime Minister presages an anti-encryption U.K. government. Prime Minister May has spoken openly about her position that companies must be able to obtain the content of messages sent on their service, and be able to give them to the relevant authorities upon request.[110] Former Prime Minister David Cameron[111] didn't back down in the face of strong criticism from industry and civil society, and it is unlikely that Theresa May will behave any differently. Although Conservatives lost their majority in the June election, the center-left parties (Labour, SNP, Liberal Democrats, and the Green Party) do not hold enough seats to form a coalition government. Instead, it is likely that the Northern Ireland-based Democratic Unionist Party (DUP) will support the Conservatives, giving a party that only holds 10 seats enormous power in the new government. The DUP's platform does not explicitly mention the IPA,[112] so we don't know how their new position of power will impact the encryption debate.

In the near term, the U.K. government is still in the process of implementing the IPA. The final versions of the Codes of Practice will soon be released, as will regulations promulgated by the government. These final documents will lay out the processes and safeguards governing the use of investigatory powers by public authorities, give detail on how those powers should be used, and provide additional clarity on compliance.[113] Section 267 of the IPA explicitly requires regulations regarding technical capability notices to be affirmatively approved by Parliament before they become binding law.[114] Codes of Practice covering the various portions of the law—including the provisions around notices—must also be affirmatively approved by Parliament.[115] Approval of both regulations and Codes of Practice are a "yes" or "no" vote, however; Parliament has no ability to amend the regulations.[116] Especially considering how the vote on the IPA played out, such a flat-out rejection of either the regulations or the Codes of Practice is unlikely, therefore opportunities to influence the implementation of the IPA through the legislative process are slim for the foreseeable future.

At this point, then, and considering both the vagueness of the law itself and the government's confusing and contradictory statements about backdoors, the IPA's impact on encryption is unclear—and a recently leaked draft of the technical capability regulation offered no new clarity. That draft confirmed that it will be the obligation of telecommunications operators to "maintain the capability to disclose, where practicable, the content of communications or secondary data in an intelligible form and to remove electronic protection applied by or on behalf of the telecommunications operator to the communications or data" when issued a warrant for that information, but that's essentially just a restatement of the law.[117] Presumably, the final version of the regulation will be equally unhelpful in resolving the question.

In the longer term, terrorist attacks, such as the ones in London on March 22, and June 3, 2017, and in Manchester on May 22, 2017, will continue to prompt policymakers to put pressure on encryption providers, and encourage broad use of the IPA's powers. Former Prime Minister Cameron's first statements about the dangers of encryption as a "means of communication" which "[the government] cannot read" came shortly after the Charlie Hebdo attacks in Paris, in response to a claim that the attackers communicated over encrypted chat.[118] Such knee-jerk reactions have occurred even around terror attacks where encryption has played no meaningful role, such as the November 2015 Paris attacks.[119] This is a trend we have seen in multiple western democracies, including the U.S., Germany, and France.[120] Given global trends of conflict and terrorism, it is a good assumption that these incidents will continue, and each one presents anti-encryption policymakers with a new opportunity to raise their concerns and link encryption to fears around terrorism.

Indeed, we have already seen an example of post-attack worry and legal uncertainty about the IPA combining in a troublesome way. Shortly after the Manchester attack in May, *The Sun* quoted unnamed government sources saying that encrypted services like Whatsapp would be receiving

technical capability notices soon after the recent election—presumably targeted at undermining their encryption, based on the headline, although the story is ultimately unclear on what would be demanded. Said one unnamed minister, "The social media companies have been laughing in our faces for too long."[121] Such stories, though troublesome, raise the possibility that despite the official secrecy surrounding technical capability notices, there may still be opportunity to learn about and debate the appropriateness of the government's demands—because policymakers won't be able to help themselves from trying to score political points by rattling their sabers in public.

Another potential impact on the future of encryption policy in the U.K. is the "Brexit" process, by which the U.K. intends to remove itself from the European Union.[122] If the government is no longer subject to European Union Court of Justice (ECJ) rulings, then the U.K. policy will no longer be constrained by that traditionally more pro-privacy and human rights-supporting legal body which has previously acted to rein in the U.K.'s most aggressive surveillance authorities.[123]

Apart from EU bodies like the ECJ, the European Convention on Human Rights (ECHR) has also had impact on U.K. surveillance authorities in the past. For example, RIPA, the pre-IPA legislation that defined encryption and surveillance powers, was introduced in part to bring the U.K.'s surveillance activities in line with past rulings of the European Court of Human Rights (which is distinct from the European Union Court of Justice).[124] However, Theresa May announced last year her intention to campaign on leaving the human rights treaty in 2020.[125] Thankfully, several factions within the Conservative party, concerned about its potential to distract from Brexit, discouraged May from including this promise in her 2017 campaign platform. Instead, she committed the U.K. to staying in the ECHR for the duration of the Brexit process.[126] However, there remains a distinct possibility that the U.K. may free itself of oversight by both the Court of Justice and the Court of Human Rights within the foreseeable future. WIthout those courts' guidance it is possible that the IPA's vague, broad provisions will be applied to dangerously undermine encryption in the U.K. and around the world without any meaningful outside check to rein the government in. This risk further highlights the need for pro-encryption advocates to cooperate internationally and keep pressure on the U.K. to avoid trying to use the IPA to force backdoors into encrypted tools used by over a billion people across the globe.

**This risk further highlights the need for pro-encryption advocates to cooperate internationally and keep pressure on the U.K. to avoid trying to use the IPA to force backdoors into encrypted tools used by over a billion people across the globe.**

# LESSONS AND STRATEGIC RECOMMENDATIONS

The legislative fight over encryption back doors in the United Kingdom appeared to be over before it even began. There were a few different causes for this that can inform how proponents of strong encryption can continue the fight both in the U.K. and elsewhere.

### 1. When fighting in Parliament on surveillance issues you need to build alliances across parties in order to make progress.

The political culture of Parliament and its multiple parties is quite different from the two-party U.S. Congress. In the U.S., members of Congress can and often do vote against their own party's leaders or form coalitions across parties, and a robust right-left coalition has emerged to defend encryption. In the U.K. system, however, a culture of party unity makes breaking with your own party very difficult, such that if the majority party or coalition of parties wants to pass a law, it's nearly impossible for minority parties to stop it. In the case of the Investigatory Powers Act, even the largest opposition party, the center-left Labour party, seemed to have no interest in fighting the Act despite some initial strong objections, in part because it is concerned about being painted as weak on crime and terrorism compared to the then-majority Conservative party, and in part due to a general alignment with and trust in the government when it comes to such issues. (This same dynamic can often be seen with centrist Democrats in the U.S. Congress.) Meanwhile, the Liberal Democrats and Scottish National Party together did not hold enough seats to seriously challenge legislation.

In future surveillance fights, building diverse coalitions of parties who support protection of privacy and digital security will be necessary for success. In the wake of the IPA, and in the context of the most recent election where the Conservatives lost their majority in the House of Commons, parties who abstained in earlier votes will need to engage in the process. A more complex Parliament, and a coalition or minority government, requires parties to collaborate and their members to urge them to do so—and highlights the possibility that a single "swing party" could make all the difference on issues of surveillance and privacy.

### 2. British voters and policymakers don't seem as concerned about government surveillance overreach as Americans (or Germans), so advocates need to focus on other arguments.

There was not a great deal of opposition to the IPA or support for encryption from the general public, nor a substantial grassroots effort to oppose the IPA's encryption-relevant provisions despite concerted effort from the local NGO community. In part, this can be attributed to a difference in culture: British residents (whose most famous modern fictional hero is a British spy) seem to have fewer qualms about government surveillance and more trust in government authority than do Americans (with their founding myth of struggle against an overbearing colonial power) or Germans (with living-memory experience with Nazi and Soviet oppression and mass surveillance), though this may not hold as true for Scottish or Northern Ireland residents. This cultural difference suggests that arguments based on the economic security or cybersecurity risks of undermining encryption will be most successful in the U.K., as they have been in the U.S. For example, NGO anti-IPA campaigning focused on how the IPA would threaten the U.K tech industry's competitiveness and undermine the security of U.K. enterprises against international corporate espionage. This may have generated positive movement in Parliament than comparing the government's spying ambitions to those of North Korea or Russia, even if such comparisons were warranted.[127]

### 3. The domestic British tech industry needs to be more deeply engaged on this issue.

The U.K.'s tech industry would have been well-placed to make the economic arguments, and did so. However, with relatively few U.K.-native corporate giants in the internet space, business arguments carried less weight than in the U.S. Speaking of the U.S., American internet companies intervened as well, but economic arguments made by non-domestic companies have less impact, and could even end up counter-productive (though less so here than in France, where animus against perceived American tech imperialism has played a much greater role in the debate). To succeed on issues like this in the future, concerted effort must be made to organize even greater engagement by both large and small ISPs as well as the small but growing tech start-up scene, in part to counterbalance the relatively conservative influence of major telecom companies that are traditionally more friendly to cooperation with government surveillance initiatives. In the U.S., collaboration and coordination between corporate and NGO defenders of encryption has been critical to beating back the push for backdoors, and such an alliance is necessary in the U.K. as well. However, finding the people and money to help make such a partnership possible will be challenging in part due to the fact that the NGOs too are in need of greater resources.

### 4. The community of digital rights-oriented NGOs focused on domestic policy in the U.K. is still small and needs more resources.

Although it has more—and more established—digital rights NGOs than Germany or France, with groups like Privacy International, Big Brother Watch, and Open Rights Group playing a critical role in the debate, the U.K. is still a decade or so behind the U.S. in terms of developing an influential and relatively well-resourced community of organizations that have both the money, membership, and political weight necessary to help sway major political outcomes domestically. Especially considering how outcomes in the U.K. could have a powerful influence on the outcome of the crypto debate in the U.S. and in Europe, it is imperative that philanthropy and industry prioritize their support of this small but increasingly crucial sector of British civil society, with an emphasis on building the ecosystem's capacity to make security and economy-based arguments in their pursuit of rights-respecting results.

### 5. The fight must continue in public—and in secret.

Now that the U.K. has already passed a law that may be deployed to demand backdoors, the fight now (mostly) moves away from Parliament—both toward the court of public opinion, and toward the secret deliberations of the Secretaries of State, the Judicial Commissioners, and ultimately the courts. That means that the key priorities for encryption defenders are: first, keeping public pressure on the Prime Minister and the Home Secretary to make it politically undesirable to apply the IPA in an expansive way to demand backdoors, and second, creating legal pressure to interpret IPA narrowly, whether by offering expert legal argument against broadly-drafted codes of conduct or implementing regulations, or—when it comes to companies served with secret capability demands that undermine—by pressing for re-review of those demands as per the IPA's processes and fighting in court if those demands aren't withdrawn.

### 6. Alternatives to encryption backdoors must be discussed...carefully.

In the U.S., the discussion amongst many policymakers has moved away from backdoors and toward other, more targeted ways of addressing government investigators' needs. For example, a key report from leaders in the U.S. House of Representatives concluded that undermining encryption was not in the national interest such that policymakers should instead focus on other options such as targeted government hacking, mandating key disclosure directly from investigative targets, or better leveraging data that's already available without backdoors.[128] Speaking generally, such a strategy—focusing on investigative alternatives to relieve pressure around backdoors—must be handled carefully, because some of those alternatives may also raise unique privacy and security risks of their own. Such a strategy deployed in the U.K. specifically may also raise some new complications, because several of the potential alternatives being discussed in the U.S.—particularly, clear authority for government hacking and mandatory key disclosure—have already been codified in the U.K. and that has not softened the push for backdoors. This highlights the importance of addressing another key need of U.K. investigators that Theresa May has made a high priority: reforming or replacing the current Mutual Legal Assistance Treaty regime so that U.K. investigators can consistently obtain the digital evidence they need, even if it is stored in the U.S. by U.S. companies. Finding a way to address this need—in a way that both satisfies the U.K. while also protecting human rights[129]—may be a necessary step toward ensuring that the U.K. does not attempt to use the IPA to force U.S. companies to build backdoors.

## 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," *Tech Crunch*, 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 "David Cameron Says New Online Data Laws Needed," BBC News, January 12, 2015, http://www.bbc.com/news/uk-politics-30778424.

7 "David Cameron Says New Online Data Laws Needed."

8 Nicholas Watt and Patrick Wintour, "David Cameron Seeks Cooperation of U.S. President Over Encryption Crackdown," *The Guardian*, January 14, 2015, https://www.theguardian.com/uk-news/2015/jan/15/david-cameron-ask-us-barack-obama-help-tracking-islamist-extremists-online.

9 Matt Burgess, "Facebook, Google, Twitter Unite to Attack 'Snoopers' Charter'," *Wired*, January 7, 2013, http://www.wired.co.uk/article/facebook-google-twitter-investigatory-powers-bill.

10 Joint Committee on the Draft Investigatory Powers Bill, Written Evidence, U.K. Parliament (February 2016): http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf.

11 Matt Burgess, "UN warns U.K.'s IP Bill 'Undermines' the Right to Privacy,'" *Wired*, March 9, 2016, https://www.wired.co.uk/article/un-privacy-ip-bill-not-compliant-international-law.

12 Elizabeth Piper, "U.K. Minister Says Encryption on Messaging Services Is Unacceptable," *Reuters*, March 26, 2017, http://www.reuters.com/article/us-britain-security-rudd-idUSKBN16X0BE.

13 The Conservative Party, "Forward Together: Our Plan for a Stronger Britain and Prosperous Future," The Conservative Party Manifesto (2017): 79, https://s3.eu-west-2.amazonaws.com/manifesto2017/Manifesto2017.pdf.

14 *See, e.g.*, Police and Criminal Evidence Act 1984 Codes of Practice, https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

15 Investigatory Powers Act Draft Code of Practice, Equipment Interference, 66.

16 Investigatory Powers Act 2016, c.25, § 253.

17 Ibid., § 253(5).

18 Unlike the U.S. Secretary of State, who deals with foreign policy, a British Secretary of State can be one of several cabinet ministers. Every British cabinet minister is a Secretary of State. In the IPA, the Secretaries who have been given powers are the Home, Defence, and Foreign ministers.

19 Investigatory Powers Act 2016, c. 25, § 253(1)(a).

20 Ibid., § 255(2).

21 Ibid., § 255(3).

22 Ibid., § 255(4).

23 Ibid., § 253(1).

24 For more information about Judicial Commissioner oversight, see infra page 9.

25 Investigatory Powers Act 2016, c. 25, § 253(5)(c).

26 "Investigatory Powers Bill Published: Minimal Changes Are Not Even Cosmetic," *Privacy International*, March 1, 2016, https://www.privacyinternational.org/node/771.

27 Open Rights Group, "Investigatory Powers Bill," Briefing for the House of Lords, https://www.openrightsgroup.org/assets/files/campaign_resources/investigatory_powers_bill/IPBill_briefing_Lords.pdf.

28 Joint Committee on the Draft Investigatory Powers Bill, Written Evidence, 75-82.

29 "David Cameron Says New Online Data Laws Needed."

30 Rob Price, "David Cameron Is Going to Try and Ban Encryption in Britain," *Business Insider*, July 1, 2015, http://www.

businessinsider.com/david-cameron-encryption-back-doors-iphone-whatsapp-2015-7?r=UK&IR=T.

31 *Baroness Shields, HL Deb 27 October 2015, vol 765, col 1086*; Kat Hall, "'Gov't Will Not Pass Laws to Ban Encryption' – Baroness Shields", *The Register*, October 28, 2015, https://www.theregister.co.uk/2015/10/28/government_will_not_pass_laws_to_ban_encryption_says_baroness_shields/; Price, "David Cameron Is Going to Try and Ban Encryption in Britain."

32 James Comey, "Director Comey Remarks at Cybersecurity Conference," *C-SPAN Video*, March 8, 2017, https://www.c-span.org/video/?424885-2/director-comey-remarks-cybersecurity-conference&start=357.

33 Daniel Severson, "The Encryption Debate in Europe," *Hoover Institution*, Aegis Paper Series No. 1702, March 20, 2017, available at http://www.hoover.org/research/encryption-debate-europe.

34 U.K. Parliament joint committees are convened for a variety of reasons. The reason in this case was because the IPA sought to consolidate and update a large number of other provisions of U.K. law. They are committees made up of members of both the House of Commons and of Lords but have no other special powers. *See*, http://www.parliament.uk/about/how/committees/joint/.

35 Joint Committee on the Draft Investigatory Powers Bill, Report, U.K. Parliament, HL Paper 93, HC 651 (February 11, 2016): 79, https://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf.

36 Investigatory Powers Act 2016, c. 25, § 253(5).

37 Matt Burgess, "Home Office Will Make 'Major' Changes to Revised Surveillance Bill," *Wired*, March 1, 2016, http://www.wired.co.uk/article/home-office-investigatory-powers-bill.

38 Investigatory Powers Act 2016, c. 25, § 253(4); Home Office, "Interception of Communications: Draft Code of Practice" (February 2017): 68, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/593748/IP_Act_-_Draft_Interception_code_of_practice_Feb2017_FINAL_WEB.pdf.

39 Phillip Le Riche, "The Investigatory Powers Bill - It's Time to Take a Closer Look," *Graham Cluey*, March 22, 2016, https://www.grahamcluley.com/investigatory-powers-closer-look/.

40 "Investigatory Powers Act 2016: Codes of Practice," Home Office, accessed May 20, 2017, https://www.gov.uk/government/consultations/investigatory-powers-act-2016-codes-of-practice.

41 Home Office, "Investigatory Powers Act 2016 Consultation: Codes of Practice" (February 2017), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/593725/IP_Act_codes_consultation_Feb2017_FINAL_WEB.pdf.

42 Home Office, "Interception of Communications: Draft Code of Practice," 67-68.

43 Home Office, "Equipment Interference: Draft Code of Practice" (February 2017), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/593753/IP_Act_-_Draft_EI_code_of_practice_Feb2017_FINAL_WEB.pdf.

44 Investigatory Powers Act 2016, c. 25, § 252.

45 Ibid., § 252(5).

46 Home Office, "National Security Notices: Draft Code of Practice" (February 2017): 5, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/593749/IP_Act_-_Draft_NSN_code_of_practice_Feb2017_FINAL_WEB.pdf.

47 Investigatory Powers Act 2016, c.25, § 255(8).

48 Ibid.

49 Ibid., § 99 et. seq.

50 Ibid., § 102.

51 Ibid., § 103.

52 Ibid., § 106.

53 Ibid.

54 Ibid., § 102.

55 Ibid, § 129.

56 Draft Code of Practice for Equipment Interference, 26.

57 Investigatory Powers Act 2016, c. 25, § 108 et. seq.

58 Ibid., § 136 et. seq.

59 Joseph Cox, "GCHQ Details Cases of When It Would Use Bulk Hacking," *Motherboard*, August 19, 2016, https://motherboard.vice.com/en_us/article/gchq-details-cases-of-when-it-would-use-bulk-hacking.

60 For more detailed information about the IPA's hacking authorities, see European Parliament Committee on Civil Liberties, Justice, and Home Affairs, Draft Report.

61 Investigatory Powers Act 2016, c. 25, §§ 227, 254.

62 Ibid., c. 1, § 23.

63 Christine Galvagna, "UK Draft Investigatory Powers Bill Would Not Provide Sufficient Oversight of Surveillance," *Center for Democracy and Technology*, January 26, 2016, https://cdt.org/

blog/uk-draft-investigatory-powers-bill-would-not-provide-sufficient-oversight-of-surveillance/.

64 Investigatory Powers Act 2016, c. 25, §§ 253(6)(a).

65 Ibid., § 257.

66 Ibid., § 243.

67 Ibid, § 242.

68 Alex Hern, "U.K. Government Can Force Encryption Removal, but Fears Losing, Experts Say," *The Guardian*, March 29, 2017, https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act.

69 Danielle Kehl, Andi Wilson, and Kevin Bankston, "Doomed to Repeat History? Lessons From the Crypto Wars of the 1990s," *New America's Open Technology Institute*, June 2015, available at https://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/.

70 Regulation of Investigatory Powers Act 2000, c. 23, § 49(2).

71 Alexander J. Martin, "Lessons From History for U.K. Home Sec Theresa May's Investigatory Powers Bill," *The Register*, March 17, 2016, https://www.theregister.co.uk/2016/03/17/snoopers_charters_a_history/.

72 Regulation of Investigatory Powers Act 2000, c. 23, § 49. John Naughton, "Theresa May's Surveillance Plans Should Worry Us All," *The Guardian*, June 12, 2016, https://www.theguardian.com/commentisfree/2016/jun/12/theresa-may-surveillance-investigatory-powers-bill-national-security.

73 Jeremy Kirk, "U.K. Data Encryption Disclosure Law Takes Effect," *PC World*, October 1, 2017, http://www.pcworld.com/article/137881/article.html.

74 Martin, "Lessons From History for U.K. Home Sec Theresa May's Investigatory Powers Bill."

75 Section III, the encryption portion of RIPA, was supposedly not activated right away because people did not start using encryption as quickly as anticipated. In July 2007 the Home Office issued a statement that said "The Government recognised concerns about how Part III would work in practice, and decided not to implement Part III before Parliament had the opportunity to consider and approve a code of practice." Section III had been controversial, especially within the private sector. Financial services and legal firms were concerned about accidental disclosure of confidential material, and the Code of Practice was introduced in part to address this. "This Month: Final RIPA to come into force," *SC Media*, August 1, 2017, https://www.scmagazine.com/this-month-final-ripa-to-come-into-force/article/553454/.

76 Cox, "How Refusing to Hand Over Your Password Can Land You in Jail." *Motherboard*, July 9, 2014, https://motherboard.vice.com/en_us/article/how-refusing-to-hand-over-your-passwords-can-land-you-in-jail.

77 "Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2013-2014," 14, available at 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.

78 Ewen MacAskill, "'Extreme Surveillance' Becomes U.K. Law With Barely a Whimper," *The Guardian*, November 19, 2016, https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper.

79 Matt Burgess, "Where the U.K.'s Political Parties Stand on the IP Bill," *Wired*, March 16, 2016, http://www.wired.co.uk/article/ip-bill-political-party-positions.

80 Thomas Newton, "How Did Labour Vote on the Investigatory Powers Act?," *PC Mag*, December 1, 2016, http://uk.pcmag.com/ip-act/86389/feature/how-did-labour-vote-on-the-investigatory-powers-act.

81 Burgess, "Where the U.K.'s Political Parties Stand on the IP Bill."

82 Ibid.

83 Samuel Barratt, "Investigatory Powers Bill Shows the Home Office Don't Understand or Care About Privacy," *Liberal Democrats* (official website), March 2, 2016, http://www.libdems.org.uk/investigatory-powers-bill.

84 Matt Burgess, "What Is the IP Act and How Will It Affect You?" *Wired*, May 8, 2017, https://www.wired.co.uk/article/ip-bill-law-details-passed.

85 Newton, "How Did Labour Vote on the Investigatory Powers Act?"

86 "Our Campaign," *Don't Spy On Us*, https://www.dontspyonus.org.uk/our-campaign.

87 "Privacy Not Prism Legal Challenge," *Privacy Not Prism*, https://www.privacynotprism.org.uk/.

88 Ibid., 92.

89 Ibid., 899.

90 The full list of organizations included is Access Now,

Advocacy for Principled Action in Government, the Center for Financial Privacy and Human Rights, the Electronic Frontier Foundation, New America's Open Technology Institute, Restore the Fourth, and TechFreedom.

91 Joint Committee on the Draft Investigatory Powers Bill, Written Evidence, 19-20.

92 Comments to the Joint Committee on the Draft Investigatory Powers Bill, *New America's Open Technology Institute*, available at https://static.newamerica.org/attachments/12257-oti-submits-comments-to-uks-draft-investigatory-powers-bill-joint-committee-on-the-importance-of-supporting-strong-encryption/OTI_Investigatory_Powers_Bill_Comment.e984a3a0fb084b539588a48d2e3dacc6.pdf.

93 Joint Committee on the Draft Investigatory Powers Bill, Written Evidence, 1316.

94 Ibid., 153.

95 Ibid., 256.

96 "Global Government Surveillance Reform," *Reform Government Surveillance*, https://www.reformgovernmentsurveillance.com/.

97 Joint Committee on the Draft Investigatory Powers Bill, Written Evidence, 387.

98 Ibid., 389.

99 Ibid., 79.

100 Ibid., 80.

101 Ibid., 1011-12.

102 The Information Commissioner's Office, "Joint Committee on the Draft Investigatory Powers Bill – Information Commissioner's submission" (2016): ¶ 37, https://ico.org.uk/media/about-the-ico/consultation-responses/2016/1560392/draft-investigatory-powers-bill-the-information-commissioners-submission.pdf.

103 Robert Hannigan, "Front Doors and Strong Locks: Encryption, Privacy and Intelligence Gathering in the Digital Era," Speech of the GCHQ Director at the Massachusetts Institute of Technology (March 8, 2016), https://www.gchq.gov.uk/speech/front-doors-and-strong-locks-encryption-privacy-and-intelligence-gathering-digital-era.

104 Joint Committee on the Draft Investigatory Powers Bill, Written Evidence, 813.

105 Ibid., 504.

106 Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," Northwestern Journal of Technology and Intellectual Property 12:1 [2014]: 1-64, available at http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip.

107 Joint Committee on the Draft Investigatory Powers Bill, Written Evidence, 638.

108 Ibid., 360-61.

109 Ibid., 1037.

110 Thomas Tamblyn, "Theresa May: The 'Snoopers' Charter' Will Not Ban Encryption," *Huffington Post*, January 12, 2016, http://www.huffingtonpost.co.uk/2016/01/14/theresa-may-the-snoopers-charter-will-not-ban-encryption_n_8976676.html.

111 Rob Price, "Why David Cameron's Encryption Ban Won't Work," *Gizmodo*, July 3, 2015, http://www.gizmodo.co.uk/2015/07/why-david-camerons-encryption-ban-wont-work.

112 "Standing Strong for Northern Ireland: DUP Manifesto for the 2017 Westminster Election," *Democratic Unionist Party*, available at http://dev.mydup.com/images/uploads/publications/DUP_Wminster_Manifesto_2017_v5.pdf.

113 Rob Price, "Why David Cameron's Encryption Ban Won't Work," *Gizmodo*, July 3, 2015, http://www.gizmodo.co.uk/2015/07/why-david-camerons-encryption-ban-wont-work.

114 Investigatory Powers Act 2016, c. 25, § 267(3).

115 Ibid., Sch. 7, ¶ 4(4).

116 *See*, Statutory Instruments - U.K. Parliament, http://www.parliament.uk/business/bills-and-legislation/secondary-legislation/statutory-instruments/.

117 Home Office, "The Investigatory Powers (Technical Capability) Regulations 2017," Draft regulations prepared by the Home Office for consultation prior to being laid before Parliament (2017), https://www.openrightsgroup.org/assets/files/pdfs/home_office/ANNEX_A_Draft_Investigatory_Powers_[Technical%20Capability]_Regulations.pdf; Matt Burgess, "Leaked Documents Reveal How the Government Will Demand Your Data Under the Snooper's Charter," *Wired*, May 5, 2017, http://www.wired.co.uk/article/uk-government-encryption-snoopers-charter.

118 Alex Hern, "How Has David Cameron Caused a Storm Over Encryption?" *The Guardian*, January 15, 2015, https://www.

theguardian.com/technology/2015/jan/15/david-cameron-encryption-anti-terror-laws.

119 Chris Smith, "Paris Attackers Didn't Use Encrypted iPhones or Internet Services," *BGR*, March 22, 2016, https://bgr.com/2016/03/22/paris-attacks-iphone-encryption/.

120 Lomas, "Encryption Under Fire in Europe As France and Germany Call for Decrypt Law."

121 Tho Newton Dunn, "Tech Giants Tamed: Ministers to Enforce New Powers to Compel Tech Giants to Hand Over Encrypted Data," The Sun, May 23, 2017, https://www.thesun.co.uk/news/3634595/ministers-to-enforce-new-powers-to-compel-tech-giants-to-hand-over-encrypted-data/.

122 Alex Hunt and Brian Wheeler, "Brexit: All You Need to Know About the U.K. Leaving the EU," *BBC News*, April 25, 2017, http://www.bbc.com/news/uk-politics-32810887.

123 Joined Cases C-203/15 and C-698/15 (Home Secretary v. Tom Watson *et. al.*) (December 21, 20016), https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/12/Watson-judgment-1.pdf.

124 The Interception of Communications Act 1985, c. 56, was enacted following the U.K. government's defeat in Malone v. United Kingdom, 82 Eur. Ct. H.R. 10 (1984), in which the ECtHR declared that non-statutory wiretaps violated Article 8 of the ECHR.

125 Will Worley, "Theresa May 'Will Campaign to Leave the European Convention on Human Rights in 2020 Election'," *The Independent*, December 29, 2016, http://www.independent.co.uk/news/uk/politics/theresa-may-campaign-leave-european-convention-on-human-rights-2020-general-election-brexit-a7499951.html.

126 Christopher Hope, "Britain to Be Bound by European Human Rights Laws for at Least Another Five Years Even If Tories Win Election," *The Telegraph*, May 18, 2017, http://www.telegraph.co.uk/news/2017/05/18/britain-bound-european-human-rights-laws-least-another-five/.

127 See, e.g., Matt Payton, "Investigatory Powers Bill: Privacy Campaigners Launch Petition Against Home Office Over New 'Snooper's Bill'," *The Independent*, May 10, 2016, http://www.independent.co.uk/news/uk/home-news/investigatory-powers-bill-privacy-campaigners-launch-petition-against-home-office-over-new-snoopers-a7022206.html.

128 House Judiciary and House Energy & Commerce Committees Encryption Working Group, Year-End Report, December 20, 2016, https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf.

129 Some proposals to address this cross-border data issue have been made, though so far the do not adequately address human rights and privacy concerns. See, e.g., Ross Schulman and Greg Nojeim, "Foreign Governments, Tech Companies, and Your Data: A Response to Jennifer Daskal and Andrew Woods," *Just Security*, August 30, 2016, https://www.justsecurity.org/32529/foreign-governments-tech-companies-data-response-jennifer-daskal-andrew-woods/.