BHAIRAV ACHARYA, KEVIN BANKSTON, ROSS SCHULMAN, ANDI WILSON

DECIPHERING THE EUROPEAN ENCRYPTION DEBATE: GERMANY

JULY 2017
(UPDATED JANUARY 2018)

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 Sven Herpig, Lisa Gutermuth, Julia Schuetze, Andrea Hackl, and our other external reviewers for their input and comments 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 **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 U.S. Governments in the U.K., Germany, France, and other European countries have recently taken steps toward undermining encryption. 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 one another, with limited sharing of information, arguments, and advocacy tactics between those countries' policy communities. This series of papers will fill in some of those gaps by recounting the legal landscape and political rhetoric in various European capitals. This is the second of those papers, focused on the encryption debate in Germany. The other papers in the series cover the encryption debates in the U.K. and France.

Contents

INTRODUCTION

Germany has a unique relationship with encryption that stands in stark contrast with that of the U.K. and France. The country doesn't have any existing laws that prohibit the use of encryption, compel users to disclose their keys, or require mandatory decryption of encrypted data. In fact, encryption has been strongly endorsed by the German government for many years. A recent series of joint letters to the European Commission from the German and French interior ministers calling for encryption controls through legislation may signify the beginning of a shift in national policy, following the trend we have seen in the U.S. and other parts of Europe.[1] Or, it may simply signify a divergence of opinion on the issue between law enforcement and other parts of the German government that have long championed encryption as an important tool for data privacy and security, similar to the U.S. government's own internal disagreements on the issue.

The legal and political landscape of surveillance in Germany, with its history of Nazi and Stasi repression,[2] is quite unlike that of the U.S., the U.K., or France. In contemporary Germany, data privacy laws are among the strongest in the world, government surveillance is strictly regulated, and the right to privacy is especially strong.[3] The German government explicitly encourages its citizens to use encryption, including end-to-end encryption systems in which only the sender and recipient can decrypt the message.[4] However, at the same time that it supports the use of strong encryption, the government conducts widespread investigatory hacking to gain access to encrypted evidence and intelligence.[5] To govern that activity, Germany has a complex legal regime that regulates the use of hacking to access data before it is encrypted[6]—a framework that was amended just last month to sharply expand the government's hacking authorities.[7]

> **The German government explicitly encourages its citizens to use encryption, including end-to-end encryption systems in which only the sender and recipient can decrypt the message.**

CURRENT LEGAL LANDSCAPE: PRO-ENCRYPTION, BUT ALSO PRO-HACKING

Germany has no laws that force disclosure of encryption keys or decryption of content, nor any laws that limit the strength or use of encryption. Instead, the government has a history of supporting the right to encrypt, promoting the use of encryption, and even attempting to create email encryption tools. However, Germany also has an extensive legal regime to enable surreptitious remote hacking into targeted devices. Law enforcement and intelligence agencies at both the federal and state level can use a wide variety of legal tools to authorize hacking activities, which are often used to bypass the challenges that encryption poses for law enforcement.[8] At the federal level, there are two intelligence agencies and three law enforcement agencies that can conduct government hacking. At the state level—Germany has 16 states (Länder)—government hacking powers are divided between state intelligence agencies and state law enforcement agencies.[9]

Law enforcement agencies in Germany conduct hacking under three major authorities, and the text of each authority uses slightly different language to refer to the act of hacking. The most explicit is the authorization contained in section 20k of the Federal Office of Criminal Investigation Act that permits law enforcement to "intervene with technical means in information technology systems."[10] The Federal Police Law, meanwhile, only refers to collecting personal data through "special means" and "technical means in a way not visible to the person concerned."[11] Finally, section 100a of Germany's Code of Criminal Procedure only authorizes the interception of communications, but German courts have interpreted a power to hack devices in the interception authority, particularly where doing so would enable collection prior to encryption.[12]

Under any of the above criminal authorities, the hacking must be approved by an independent judge. Under the Code of Criminal Procedure, the crime must be one of a specified set of serious crimes, while under the Federal Office of Criminal Investigation Act authorization is limited to danger to life and limb or to the security of the nation. Device owners are also entitled to notice of the hacking as soon as notice can be effected.[13] Finally, all of the laws also contain restrictions on the collection of "core areas" information, which must not be collected and must be deleted immediately if inadvertently gathered. "Core areas" are those defined in Articles I and II of the Basic Law and

describe a highly private area for the individual which is free from surveillance. The doctrine of core areas has its roots in the fundamental rights found in Articles 1 and 2 of Germany's Basic Law,[14] ensuring a core of human dignity that is typically beyond the state's reach. For example, core areas include communications between close family members, as well as communications with outside individuals such as defence counsel, doctors, and clergy.[15] The authorizations for intelligence agencies' hacking, of which there are also three, are even more vague, referring only to collecting data "which has been stored."[16]

As applied by the courts, the core areas doctrine has led to two major legal limits on the government's ability to hack into and search an entire device for either law enforcement or intelligence reasons. Such a search is often referred to as an "online search" and is distinct from "source telecommunication surveillance," (quellen TKÜ) which is restricted to retrieving the content of messages as they are being typed– ongoing communication. These limitations on online searches are a result of two legal cases, the Online Search and Counterterrorism cases, which will be discussed later in this paper. First, hacking can only be performed when there is a specific impending danger to human lives and the German state.[17] Second, an independent body must ensure that "core area" (Kernbereich privater Lebensgestaltung, or simply Kernbereich) information is not collected.[18] Taken together, these limitations and safeguards constitute the German equivalent of strict scrutiny review. In addition to these constitutional limits, requests for authorization to hack must include certain data indicators, which vary by authorizing statute. For example, the Code of Criminal Procedure requires data relevant to the identity and location of the person (where known), the telephone number or other code equipment, and the type, extent and duration of the measure.[19]

Finally, it is important to note that some of the above authorities were amended and broadly expanded in late June 2017, as this paper was being finalized. The debate over the change and its implications are discussed below, but two major changes are worth noting here: first, the limitations on usage of online searches were relaxed to include a much larger list of crimes, and second, source telecommunication surveillance was officially codified and authorized in statute for the first time.[20]

Germany's intertwined support of both strong encryption and robust investigatory hacking is the result of years of evolution in Germany's public policy discussions. We turn next to a discussion of the history of that debate.

HOW DID WE GET HERE, AND WHAT MAY THE FUTURE HOLD?

A Tradition of Supporting Encryption

Germany's strong stance on encryption goes back many years. As early as 1991, Germany split its cryptography research unit away from its intelligence agency and turned it into its own Federal Office for Information Security.[21] Later that decade, in 1999, the German government enacted an official policy on cryptography that broadly endorsed the use and development of encryption, opposed bans or limitations on technology, and called for other technical means to address the challenges of law enforcement,[22] roughly mirroring the conclusion of the "crypto wars" that occurred in the U.S. in the 1990s.[23]

Germany continues to officially support the use of strong encryption by its citizens today. The Digital Agenda 2014-2017, a white paper on Germany's digital policy, states that the German government "support[s] the use of more and better encryption and aim[s] to be the world's leading country in this area. To achieve this goal, the encryption of private communication must be adopted as standard across the board."[24] The Digital Agenda goes on to declare that "it is the common duty of industry, science, and policy makers to establish secure information systems and to make these available for the common good,"[25] and therefore the government "support[s] and demand[s] the use of trustworthy IT security technologies, especially the use of more and better encryption in electronic communication."[26] Similarly, the 2015 Charter to Strengthen Trusted Communications declared, "We [Germany] want to be the No. 1 encryption site in the world. We believe in trustable communications, particularly end-to-end encryption."[27] The Charter, which was signed by representatives of the government and the private sector, was designed to encourage private companies, particularly startups, to create an encryption-focused, innovative digital economy in Germany.

Consistent with that mandate, the German government has sanctioned and encouraged the use of De-Mail, an electronic communication service that uses encryption technology.[28] Although it was initially criticized for its security flaws—malware scanning processes meant that the messages could not be encrypted end-to-end—in 2015 it enabled end-to-end email encryption via easy-to-use webmail plugins using the well-tested OpenPGP standard.[29] The government's support of De-Mail, and the inclusion of encryption requirements in various laws and regulations, shows that the government recognizes the crucial role that strong encryption can play in modern communications.[30]

However, despite this strong history of support for encryption, some members of the German government are beginning to question the policy. In 2015, German Interior Minister Thomas de Maizière called for the ability to "decrypt or bypass encrypted communication."[31] The following year, in the wake of a series of terrorist attacks in Paris, Brussels, and Nice, the minister and his French counterpart made a joint statement calling for action in the face of increasing use of encryption technologies.[32] They proposed that the European Commission examining the possibility of a directive requiring operators offering telecommunications or internet products or services in the European Union to remove illegal content or to decipher messages in the course of investigations.[33] Other German government officials from the Christian Democratic Union party made similar statements.[34] In February 2017, De Maizière and the French interior minister sent a joint letter to the European Commission regarding potential Europe-wide legislation requiring communications providers to be able to decrypt user information upon request.[35] Although there were certain discrepancies between the published French and German letters, pressure to address concerns about encryption led to a European Commission study on the use of encryption tools. The study will propose new measures to address the challenges encryption poses to government investigators.[36]

The contradiction between De Maizière's position and that of the wider government has not been lost on others. Konstantin von Notz, internet policy spokesman for the Green Party, pointed out: "Mr. de Maizière wants to make Germany the number one encryption country, but he does not want any end-to-end encryption. He wants to strengthen IT security, but sticks to [government hacking]. This is counterproductive."[37] This same tension is reflected in the the government's 2016 cybersecurity strategy, which sought to promote both "security through encryption" and "security despite encryption."[38] As experts at the German tech policy think tank Stiftung Neue Verantwortung (SNV) describe: "For the German government this apparent contradiction can be resolved through lawful hacking."[39] A focus on government hacking instead of mandating that providers build intentional vulnerabilities into product's encryption technology to enable third parties to decrypt encrypted data (i.e., "backdoors") has "allow[ed] the main pillar of German crypto policy—the support and promotion of strong encryption technologies—to remain in place" while "provid[ing] possibilities to gain access even if encryption is employed."[40] While similar arguments have been made in the context of the U.S. encryption debate, where some advocates and policymakers have pointed to hacking as a more targeted solution to investigators' needs than backdoors,[41] the German example provides a cautionary tale: after a decade of court fights and policy debates, Germany just considerably expanded its lawful hacking authority through new legislation allowing secret remote exploitation of computing devices in the investigation of a wide range of regular crimes.

A History of Hacking

The German government has long viewed remote hacking of targeted computers as a useful tool to gain access to information that might otherwise be unobtainable due to encryption,[42] or even just due to the inefficiencies of the Mutual Legal Assistance Treaty system for making law enforcement data requests to online service providers based abroad.[43] Law enforcement has been hacking in Germany since at least 2005, when its use was first revealed.[44] Both intelligence and law enforcement agencies at the state and federal levels were then (and are now) using hacking tools in their investigations.[45]

Throughout the past decade, courts in Germany have been considering the use of hacking and the rules and procedures surrounding it. In the landmark 2008 Online Search case, the Constitutional Court (Germany's highest court for constitutional review) examined a particular state's intelligence agency's hacking powers as laid out in the law of the state of North-Rhine Westphalia. The court concluded that intruding into an individual's device was an inherently disproportionate form of surveillance which intruded into the "core areas" of people's private lives and was unconstitutional if

not specially authorized and subjected to particular limits and safeguards.[46] In essence, the court declared that Germans have a fundamental right to the integrity of their data and computers. Therefore hacking is only permissible, according the court, if performed in response to threats to life or to the state itself and subject to frequent review to ensure that unnecessary, disproportionate, or core area information was not collected.[47]

Law enforcement has continued to conduct investigative hacking activities since the Online Search case, often without seeking the specific authorizations and safeguards called for by the Constitutional Court. Instead, German authorities have been relying on a narrower form of hacking known as "source telecommunication surveillance"—that is, the interception of communications on the target's device before they have been sent (or encrypted). Germany's Telecommunications Law of 1996, the requirements of which are less stringent than those in the Online Search case, covers the real time surveillance of all types of voice and electronic communications.[48] The German government has therefore chosen to argue in the wake of Online Search that communications sitting on a target's device waiting to be sent are "telecommunications" covered by that law such that, e.g., secretly implanting software to capture the text of an email or text message while it is being typed and before it has been sent (or encrypted) is just another kind of surveillance that can be authorized under that law.[49]

The New Wave of Government Hacking

Despite the restrictions that came out of the Constitutional Court's 2008 decision in Online Search, by the end of that same year new anti-terror legislation was passed that aimed to substantially increase the scope of Germany's hacking activities. That legislation was championed by Wolfgang Schäuble, the former interior minister in Chancellor Angela Merkel's cabinet, who in 2006 began promoting the controversial Program to Strengthen Internal Security, which would increase funding for German intelligence and law enforcement agencies to improve their hacking abilities. The proposed program would task the Federal Criminal Investigation Agency (BKA), Germany's version of the Federal Bureau of Investigation, with using these new hacking powers to counter terrorism.[50] In the past there were concerns that Germany's surveillance regime, which had faced opposition stemming from the country's history of fascism, was too diffuse to effectively detect plots and prevent attacks.[51] Centralizing counterterrorism hacking authorities under one agency, Schäuble argued, was a way of addressing these concerns. In 2008 Schäuble introduced a bill, which amended the Federal Criminal Police Office Act (the BKA Law) to extend law enforcement's ability to conduct online searches, video surveillance of homes, and phone monitoring.[52] The proposal was criticized by opposition parties[53] and civil liberties advocates who were highly concerned that the growing convergence of even greater powers in one agency threatened to create a "super authority" secret police organization.[54]

Schäuble's bill weathered civil society condemnation, political opposition, and even survived a failure in the Federal Council[55] before it was enacted in December 2008. The BKA law was soon challenged in the Constitutional Court, from which it emerged in 2009 with minor restrictions. Schäuble's bill once again faced a Constitutional challenge years later in the Counterterrorism case, which resolved in April 2016 with new limitations on the government's ability to hack in anti-terrorism investigations.[56] As it did in the Online Search decision, the court found that hacking was a special legal measure that could be used, with strict safeguards, to protect national security and public safety. As long as government hacking respected the core areas doctrine and adhered to other safeguards, it was declared permissible.[57] However, this decision also urged the government to further clarify the statutory authority for lawful hacking by June 2018.

The BKA is not the only agency that has seen its hacking powers expanded. The German government has also expanded funding for a variety of agencies

with hacking powers. In 2017, Chancellor Merkel announced that half a billion euros would be invested in the Federal Intelligence Service, Germany's primary intelligence agency, to ramp up its technical capabilities.[58] The exact purpose of the budgetary increase is secret, but news reports suggest that up to 150 million euros will be spent to undermine encrypted messaging services like WhatsApp.[59] The Federal Constitution Protection Office, which is tasked with monitoring extremism, similarly received funds to improve its ability to cooperate with the U.S. National Security Agency and monitor internet communications.[60]

The German government continued to double down on hacking as an investigative and intelligence technique by creating and investing in brand new agency actors specifically focused on it. In April 2017, a new military cyber command intended to give the German government offensive hacking capabilities became operational.[61] The same year the government announced the creation of a new cryptanalysis agency, the Central Office for Information in the Security Sphere (ZITiS), to fulfill Interior Minister de Maizière's calls for a "cybersecurity offensive" against hostile actors.[62] Besides monitoring the internet and working to undermine encryption, ZITiS will be a clearinghouse for expertise on government hacking.[63] These changes did not come without significant criticism, however. The Green Party called ZITiS a "constitutionally highly questionable initiative" and former data protection commissioner Peter Schaar expressed concern that it lacks legal legitimacy, and that there will be no possibility for review by the Federal Constitutional Court.[64]

Such debates over hacking in Germany are far from over, with new developments and heated argument occurring to this day. As this paper was being prepared, an amendment to a bill covering effective law enforcement was introduced in the Bundestag that would massively alter and expand the legislative authority under which the German government conducts hacking. The amendment—which passed, along with the broader bill, on June 22, 2017—was introduced at the last minute, drawing criticism based on both its procedure and content. The new law expands both the "online search" and "source telecommunication surveillance" powers. The online search authorization—the ability to capture every piece of data on a device—was broadened to cover 27 different serious crimes instead of solely situations of international terrorism and risk to life and limb. The new law also officially codified and authorized the source telecommunication surveillance practice, officially instituting a test based on necessity, proportionality, and technical feasibility, allowing its use in relation to an expanded list of 38 different crimes.

Many members of the opposition parties in Germany have raised concerns with the new provisions, including serious questions about its constitutionality in the face of the Online Search case and others. Civil society in Germany has also been critical. Organizations like the Chaos Computer Club, Forum Privatheit, and Gesellschaft für Informatik have been joined by the legal community and the Green Party in questioning the constitutionality of the new law.[65] Prof. Dr. Hartmut Pohl, from Gesellschaft für Informatik, said that the expanded provisions in the new law represent an impermissible intrusion into privacy and fundamental rights. He also warned that it is not yet clear how the measure could be designed to ensure the protection of the core area of private life design, which has been declared indispensable by the Federal Constitutional Court.[66] Constitutional challenge to the new authorities is almost assured, so the federal courts in Germany will likely have the next word on Germany's consistent and continued drive toward conducting more, and more extensive, government hacking.

LESSONS LEARNED AND STRATEGIES FOR ACTION

1. Germany is relatively receptive to privacy-based arguments around encryption.

In Germany, the right to privacy flows from the inviolable rights to human dignity and personality, among others. According to German law, to be an 'informationally self-determining person,' as opposed to a mere object of the state, a person must be able to make sovereign decisions about one's privacy. That includes the right to encrypt one's data. Therefore, the absence of encryption backdoors, compulsory key disclosure, or mandatory decryption laws is a direct consequence of Germany's unique conception of privacy, strongly informed by its Nazi history and East Germany's experiences under Stasi surveillance. Consequently, Germany seems much more open to privacy-based arguments around encryption than the U.K., France, and even the U.S. At the same time, the country is no stranger to terrorism and national security threats, having suffered radical left-wing terrorism, neo-Nazi terrorism, and Islamist terrorism while being, for most of its modern existence, a Cold War front. Germany's experience thereby teaches the world that a strong conception of privacy can weather even persistent security threats.

2. Germany is also very open to economic and cybersecurity arguments in favor of encryption.

Germany has long prided itself on being a global industrial leader, and as reflected in the federal government's Digital Agenda 2014-2017 white paper, it intends to maintain its role as a digital leader as well. As a result, the German government has explicitly recognized that maintaining strong cybersecurity—including through strong end-to-end encryption—is critical to maintaining its economic security in the 21st century. In addition to compelling economic arguments, Germany has had another reason to be concerned about its cybersecurity: Edward Snowden's revelations about the National Security Agency's (NSA) global web of internet surveillance, which captured the communications of—among others—German Chancellor Angela Merkel herself. Therefore, post-Snowden concern about foreign intelligence agencies—as well as concern about economic espionage—has been a strong driver for encryption adoption. As Germany embraces arguments based on privacy, economics, and cybersecurity, it provides a model for how other governments could sensibly approach encryption. Strikingly, though, its rejection of encryption backdoors as a matter of policy didn't turn so much on corporate or civil society engagement but instead on the engagement of different parts of the government.

3. Government offices and agencies that are focused on privacy, security, and commerce can successfully counter law enforcement agencies' call for backdoors.

In the U.S., although former FBI Director James Comey aggressively campaigned against encryption, he was restrained by the Obama White House which had chosen not to pursue legislation on the issue. It made that choice in no small part because the privacy watchdogs at the Federal Trade Commission, as well as the Commerce Department concerned with U.S. tech competitiveness, the State Department concerned with securing internet freedom and human rights globally, and elements of the Department of Homeland Security and the Intelligence Community responsible for cybersecurity defense, all pushed back on the FBI. Similarly, government watchdogs and regulatory bodies in Germany—particularly its data protection authorities, at both the federal and state levels—have vocally supported encryption.

Besides checking the government's powers, the data protection authorities sanction communications service providers that offer inadequate security, educate the public on which communications services providers they should use, offer encryption-specific guidance to app developers and crypto startups, and play a large role in incubating the domestic encryption industry which has rapidly expanded after the Snowden leaks. Because the data protection authorities are influential, their concerns are frequently mirrored by other powerful institutions. This growing and multifarious body of sentiment across the different parts of government helps to ensure that even when law enforcement officials go against broader government policy and start agitating around backdoors—whether it's the U.S. FBI director or Germany's interior minister—their impact is limited. Ultimately, the role of Germany's data protection authorities in the encryption debate—like the role of the various agencies in the U.S. debate—highlights how important it is for parts of government other than law enforcement to engage in the encryption debate to defend their own institutional interests.

4. Lawful hacking can be a political and practically workable alternative to backdoors, but raises its own privacy and security challenges.

Germany's growing focus on investigative hacking, both in terms of clarifying legal authority and increasing budgetary resources, demonstrates how such a focus can take pressure off the encryption debate and facilitate a move away from discussion of backdoors. This is, to some extent, a positive development. Targeted hacking of particular suspects using existing vulnerabilities is, on balance, much better from a privacy and security perspective than mandating backdoors (i.e., requiring that new vulnerabilities be engineered into every product to facilitate government exploitation). This pivot in the German discussion can and should be used as an example in other countries, including in the U.S. where key legislators are starting to look at lawful hacking as both an alternative to backdoors and as an area of government practice in dire need of clearer regulation. However, such a change in focus brings a new challenge and opportunity: to leverage the encryption-prompted conversation around government hacking to strengthen regulation of the practice and make it as rights-respecting as possible, rather than foster unrestrained expansion of the practice in ways that could harm privacy and security. Unfortunately, recent legislation that broadly expanded government hacking authority in Germany signals a worrisome trend in the opposite direction. Therefore, the next few years in Germany and in the U.S. are likely to be critical in terms of shaping transatlantic norms around government hacking, and cross-border multistakeholder efforts to help make those norms as strong as possible—such as German think tank Stiftung Neue Verantwortung's Transatlantic Cyber Forum, which will be tackling the hacking issue[67]—will be all the more important.

5. A strong culture of "hacktivism" and hacker collectives can bring much-needed publicity and technical expertise to issues of encryption and government hacking.

Although there are some local actors like media outlet Netzpolitik.org,[68] advocacy group Digitale Gesellschaft,[69] and Berlin offices of organizations Transparency International[70] and Amnesty International,[71] in comparison to the U.S., Germany does not have a long tradition or large ecosystem of legal and policy NGOs focused on digital rights issues. That said, the digital rights NGO scene in Berlin is quickly growing and evolving, and Germany also benefits from its long-running and robust subculture of hacker collectives such as the world-famous Chaos Computer Club,[72] which plays a key role in publicizing and explaining key aspects of the German government's surveillance and hacking operations. For example, the first revelations of government hacking in Germany arose from a series of investigations by Chaos Computer Club in 2006-07. In 2011, Germany's most high-profile hacking scandal—the use of insecure and unconstitutionally invasive malware—was a result of Chaos Computer Club's analysis of government-hacking Trojans.[73]

The group has also mobilized encryption experts and advocates, not just from Germany but around the world, which in turn leads to political action, technical progress, and greater coordination amongst the pro-encryption community. America's broad community of information security experts from academia and industry has played a similarly vocal role in the U.S. debate, but France and the U.K. have unfortunately not benefited from the same level of technical engagement and expertise. This may be a key reason why pro-encryption advocates have not been as successful in those countries.

6. U.S./German alignment on encryption may help counter the U.K./French trend against encryption.

Since Germany is easily the most pro-encryption environment of the three European countries surveyed, it is important to consider how U.S. and German policymakers and advocates who are pro-encryption might best collaborate on the issue to counter the British and French push toward backdoors, and invest resources accordingly. Any such collaboration must also focus on aggressively countering any moves against encryption in Germany, by the interior minister or otherwise, so that this strategically critical pro-encryption bulwark remains as a strong example for other European nations. Some U.S./German multi-stakeholder dialogues on these and similar issues have already occurred or are in process, such as the previously-mentioned Transatlantic Cyber Dialogue and the German Marshall Fund's Transatlantic Digital Dialogue, which concluded in its final report that U.S./German alignment would be critical to the future of encryption in Europe.[74]

Notes

1 Thomas de Maizière and Bruno La Roux, Letter to the European Commission, February 20, 2017, https://regmedia.co.uk/2017/02/28/french_german_eu_letter.pdf.

2 Thomas Coombes, "Lessons from the Stasi," *The European*, April 1, 2015, http://www.theeuropean-magazine.com/thomas-coombes/9982-the-stasi-legacy-and-its-impact-on-modern-surveillance.

3 Alvar C.H. Freude and Trixy Freude, "Echoes of History: Understanding German Data Protection," Newpolitik, October 2016, http://www.bfna.org/sites/default/files/publications/Echoes_of_history_Understanding_German_Data_Protection_Freude.pdf.

4 David Meyer, "Germany Pushes for Widespread End-to-end Email Encryption," *Gigaom*, March 9, 2015, https://gigaom.com/2015/03/09/germany-pushes-for-widespread-end-to-end-email-encryption/.

5 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.

6 Thomas de Maizière and Bruno La Roux, Letter to the European Commission, February 20, 2017, https://regmedia.co.uk/2017/02/28/french_german_eu_letter.pdf.

7 Carla Bleiker, "New Surveillance Law: German Police Allowed to Hack Smartphones," *Deutsche Welle*, June 22, 2017, http://www.dw.com/en/new-surveillance-law-german-police-allowed-to-hack-smartphones/a-39372085.

8 Herpig and Heumann, "Germany's Crypto Past and Hacking Future."

9 For example, see the state of Bavaria's primary government hacking powers. Bayerisches Verfassungsschutzgesetz [Bavarian Constitution Protection Law], July 12, 2016, GVBl. at 145, §§ 9, 10; Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei [Bavarian Police Law], September 14, 1990, GVBl. at 397, § 34d.

10 Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten [Federal Office of Criminal Investigation Act], July 7, 1997, BGBl. I at 1650, § 20k.

11 Bundespolizeigesetz [Federal Police Law], October 19, 1994, BGBl. I at 2978-79, §§ 28, 28a.

12 European Parliament Directorate-General for Internal Policies, "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices," March 2017, 79, available at http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

13 §101(5)

14 Artikel. 1. sec. 1 GG, available at https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0021.

15 cf. BVerfGE 109, 279 <321 et seq.>

16 Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz) [Federal Constitutional Protection Act], December 20, 1990, BGBl. I at 2954, 2970, § 8a; Gesetz über den Bundesnachrichtendienst (BND-Gesetz) [Federal Intelligence Act], December 20, 1990, BGBl. I at 2954, 2979, § 3; Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz) [G10 Law], June 26, 2001, BGBl. I at 1254, 2298, § 1.

17 "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices," 79; available at http://www.linguee.de/deutsch-englisch/

18 Ibid.

19 "Legal Frameworks for Hacking by Law Enforcement," 80.

20 Carla Bleiker, "New Surveillance Law: German Police Allowed to Hack Smartphones", *Deutsche Welle*, June 22, 2017, http://www.dw.com/en/new-surveillance-law-german-police-allowed-to-hack-smartphones/a-39372085.

21 Herpig and Heumann, "Germany's Crypto Past and Hacking Future."

22 "*Pressemitteilung des Bundesministerium des Innern und Bundesministerium für Wirtschaft und Technologie: Eckpunkte der deutschen Kryptopolitik*," June 2, 1999, available at https://hp.kairaven.de/law/eckwertkrypto.html.

23 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/.

24 The Federal Government, *Digital Agenda* 2014-2017 (August 2014): 31, https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda-engl.pdf.

25 The Federal Government, *Digital Agenda* 2014-2017 (August 2014): 5, https://www.digitale-agenda.de/Content/DE/_

Anlagen/2014/08/2014-08-20-digitale-agenda-engl.pdf.

26 The Federal Government, *Digital Agenda* 2014-2017 (August 2014): 32, https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda-engl.pdf.

27 "Charta zur Stärkung der vertrauenswürdigen Kommunikation," November 18, 2015, available at https://www.krypto-charta.de/charta.html.

28 "De-mail, Safe As a Letter or a Registered Mail," *Email Made in Germany*, https://www.e-mail-made-in-germany.de/De-Mail.html.

29 "De-Mail - Simply Encrypted and Verifiable," *Bundesministerium des Innern*, http://www.cio.bund.de/Web/DE/Innovative-Vorhaben/De-Mail/de_mail_node.html; David Meyer, "Germany Pushes for Widespread End-to-end Email Encryption," *Gigaom*, March 9, 2015, https://gigaom.com/2015/03/09/germany-pushes-for-widespread-end-to-end-email-encryption/.

30 Herpig and Heumann, "Germany's Crypto Past and Hacking Future."

31 Thorsten Benner, Mirko Hohmann, "The Encryption Debate We Need," *Global Public Policy Institute*, May 19, 2016, http://www.gppi.net/publications/data-technology-politics/article/the-encryption-debate-we-need/.

32 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/.

33 "Initiative Franco-allemande Sur la Sécurité Intérieure en Europe," *Le Ministère de l'Intérieur*, August 23, 2016, https://www.interieur.gouv.fr/Archives/Archives-des-actualites/2016-Actualites/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe.

34 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/.

35 Letter to the European Commission from the French and German Interior Ministers, February 20, 2017, available at https://regmedia.co.uk/2017/02/28/french_german_eu_letter.pdf. This sentence was revised in January 2018. Some articles identified discrepancies between the French language and German language versions, however, the German text was not available at the time of this revision (January 2018). See "Innenminister fordern Hintertüren gegen Verschlüsselung – in der französischen Version der gemeinsamen Erklärung (Update)," Netzpolitik.org, August 23, 2016. https://netzpolitik.org/2016/innenminister-fordern-hintertueren-gegen-verschluesselung-in-der-franzoesischen-version-der-gemeinsamen-erklaerung/.

36 Catherine Stupp, "EU to propose new rules targeting encrypted apps in June," *Euractiv*, Mar. 29, 2017, https://www.euractiv.com/section/data-protection/news/eu-to-propose-new-rules-on-police-access-to-encrypted-data-in-june/, but see Encryption, EU Commission Migration and Home Affairs, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/encryption_en [listing the second half of 2017 as a target date for delivering options].

37 Deutscher Bundestag [German Parliament], Plenary Protocol 18/60, Stenographic Report, 60th Session, October 16, 2014, https://www.bundestag.de/blob/336828/8fae96f50138b6722c09af8b5f1a44c8/18060-data.txt.

38 Herpig and Heumann, "Germany's Crypto Past and Hacking Future."

39 Ibid.

40 Ibid.

41 Bellovin, Steven M., 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, no. 1 (April 2014): 1-64, available at http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip; "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies," The White House, December 12, 2013, available at https://www.whitehouse.gov/sites/default/files/ docs/2013-12-12_rg_final_report.pdf.

42 Herpig and Heumann, "Germany's Crypto Past and Hacking Future."

43 For more information on the issues facing the Mutual Legal Assistance Treaty system, see https://www.accessnow.org/mlat-a-four-letter-word-in-need-of-reform/.

44 109 BVerfGE 279 (2004). *See also* Nicolas Nohlen, "Germany: The Electronic Eavesdropping Case," *International Journal of Constitutional Law* 3, no. 4 (2005): 680-686.

45 "Geheimdienste spitzeln schon seit Jahren," *Stern*, April 25, 2007, http://www.stern.de/digital/online/online-durchsuchungen-geheimdienste-spitzeln-schon-seit-jahren-3358202.html.

46 120 BVerfGe 274 (2008).

47 Monika Ermert, "German High Court Defines New "IT Basic Law" Curbing Online Searches", *Intellectual Property* Watch, Jan. 3, 2008, https://www.ip-watch.org/2008/03/01/german-high-court-defines-new-it-basic-law-curbing-online-searches/.

48 Telekommunikationsgesetz (TKG) § 66, v. 1.8.1996 (BGBI. I S.1120).

49 German Parliament, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Gisela Piltz et al [Answer of the Federal Government to the Question of Gisela Piltz et al], Drucksache [Printed Matter] 16/6885, October 30, 2007, http://dipbt.bundestag.de/dip21/btd/16/068/1606885.pdf; Deutscher Bundestag [German Parliament], Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Gisela Piltz et al [Answer of the Federal Government to the Question of Gisela Piltz et al], Drucksache [Printed Matter] 16/7279, November 27, 2007, http://dipbt.bundestag.de/dip21/btd/16/072/1607279.pdf.

50 "Schäuble will Online-Durchsuchung ohne richterliche Genehmigung," *Frankfurter Allgemeine*, August 31, 2007, http://www.faz.net/aktuell/politik/innere-sicherheit-schaeuble-will-online-durchsuchung-ohne-richterliche-genehmigung-1464413.html.

51 Mark Landler, "Bomb Plot Shocks Germans Into Antiterrorism Debate," *New York Times*, August 22, 2006, http://www.nytimes.com/2006/08/22/world/europe/22germany.html.

52 "Germany to Give Police More Surveillance Powers," *New York Times*, June 4, 2008, http://www.nytimes.com/2008/06/04/world/europe/04iht-04germany.13456955.html; "Datenschützer Zeichnen Schäuble Aus," Der Spiegel, October 16, 2009, http://www.spiegel.de/netzwelt/netzpolitik/big-brother-awards-datenschuetzer-zeichnen-schaeuble-aus-a-655665.html.

53 Harald Neuber, "Schritt Zu Einem Deutschen Fbi Und Zum Präventionsstaat," *Telepolis*, November 13, 2008, https://www.heise.de/tp/features/Schritt-zu-einem-deutschen-FBI-und-zum-Praeventionsstaat-3420765.html.

54 "Wolfgang Schäuble wehrt Kritik am BKA-Gesetz ab," *Die Welt*, June 4, 2008, https://www.welt.de/politik/article2065649/Wolfgang-Schaeuble-wehrt-Kritik-am-BKA-Gesetz-ab.html.

55 "Schäubles BKA-Gesetz Scheitert Im Bundesrat," *Der Spiegel*, November 28, 2008, http://www.spiegel.de/politik/deutschland/terrorabwehr-schaeubles-bka-gesetz-scheitert-im-bundesrat-a-593284.html.

56 BVerfG, Judgment of the First Senate of April 20, 2016, 1 BvR 966/09.

57 Marvin Strathmann, "Wer wird ab jetzt überwacht?," *Zeit Online*, February 22, 2016, http://www.zeit.de/digital/datenschutz/2016-02/staatstrojaner-bundestrojaner-bka-quellen-tkue; Reiko Pinkert, Jan Lukas Strozyk and Hans Leyendecker, "Bundestrojaner für Smartphones und Tablets," *Süddeutsche Zeitung*, September 30, 2016, http://www.sueddeutsche.de/politik/bundeskriminalamt-bundestrojaner-fuer-smartphones-und-tablets-1.3186711; Andre Meister, "Kritik vom Bundesrechnungshof: Das Bundeskriminalamt will gleich zwei Staatstrojaner einsetzen," *Netzpolitik*, August 15, 2016, https://netzpolitik.org/2016/kritik-vom-bundesrechnungshof-das-bundeskriminalamt-will-gleich-zwei-staatstrojaner-einsetzen/.

58 Die Bundeskanzlerin [The Chancellor's Office], "Rede von Bundeskanzlerin Merkel beim Festakt zum 60-jährigen Bestehen des Bundesnachrichtendienstes am 28. November 2016 in Berlin," Budget Speech of the German Chancellor, November 28, 2016, https://www.bundeskanzlerin.de/Content/DE/Rede/2016/11/2016-11-28-rede-bk-bnd.html.

59 Patrick Beuth, "Wir wollten ja staatliche Hacker," *Zeit Online*, November 29, 2016, http://www.zeit.de/digital/datenschutz/2016-11/verschluesselung-bnd-whatsapp-aniski-150-millionen; Andre Meister, "Projekt „ANISKI": Wie der BND mit 150 Millionen Euro Messenger wie WhatsApp entschlüsseln will," *Netzpolitik*, November 29, 2016, https://netzpolitik.org/2016/projekt-aniski-wie-der-bnd-mit-150-millionen-euro-messenger-wie-whatsapp-entschluesseln-will/; Andre Meister, "Strategische Initiative Technik: Wir enthüllen, wie der BND für 300 Millionen Euro seine Technik aufrüsten will," *Netzpolitik*, September 21, 2015, https://netzpolitik.org/2015/strategische-initiative-technik-wir-enthuellen-wie-der-bnd-fuer-300-millionen-euro-seine-technik-aufruesten-will/.

60 Antonius Kempmann, Reiko Pinkert and Jan Strozyk, "Geheimdienste bekommen mehr Millionen fürs Mitlesen," *Süddeutsche Zeitung*, September 7, 2016, http://www.sueddeutsche.de/politik/bnd-und-verfassungsschutz-geheimdienste-bekommen-mehr-millionen-fuers-mitlesen-1.3152028.

61 Sven Herpig, "Zurückhacken ist keine Lösung," *Zeit Online*, April 21, 2017, http://www.zeit.de/digital/internet/2017-04/cyberangriffe-bundesregierung-hackback-gegenangriff/komplettansicht.

62 Esther King, "Security Chief: Germany Must Go on Cybersecurity Offensive," *Politico*, January 10, 2017, http://www.politico.eu/article/security-chief-germany-must-go-on-cybersecurity-offensive/.

63 Herpig and Heumann, "Germany's Crypto Past and Hacking Future."

64 Marcus Decker, "Entschlüsselung: Bundesregierung plant neue Behörde für Überwachungstechniken," *Berliner Zeitung*,

June 24, 2016, http://www.berliner-zeitung.de/politik/entschluesselung-bundesregierung-plant-neue-behoerde-fuer-ueberwachungstechniken-24289670.

65 Andre Meister, "Staatstrojaner: Bundestag hat das krasseste Überwachungsgesetz der Legislaturperiode beschlossen", *Netzpolitik.org*, June 19, 2017, https://netzpolitik.org/2017/staatstrojaner-bundestag-beschliesst-diese-woche-das-krasseste-ueberwachungsgesetz-der-legislaturperiode/.

66 "GI kritisiert Einführung der Online-Durchsuchung in Strafprozessordnung," Gesellschaft für Informatik, June 20, 2017, https://www.gi.de/nc/aktuelles/meldungen/detailansicht/article/-1ead86c945.html.

67 "Transatlantic Cyber Forum," *Stiftung Neue Verantwortung*, available at https://www.stiftung-nv.de/en/project/international-cyber-security-policy#erstens; Sven Herpig, "Government Hacking: Computer Security vs. Investigative Powers," *Transatlantic Cyber Forum*, June 2017, availble at https://www.stiftung-nv.de/sites/default/files/snv_tcf_government_hacking-problem_analysis.pdf.

68 "About Us," *Netzpolitik.org*, https://netzpolitik.org/ueber-uns/.

69 "About Us," *Digitale Gesellschaft*," https://digitalegesellschaft.de/uber-uns/.

70 What is Transparency International?" *Transparency International*, https://www.transparency.org/about/.

71 "What We Do," *Amnesty International*, https://www.amnesty.org/en/what-we-do/.

72 *Chaos Computer Club*, https://www.ccc.de/en/home.

73 "Chaos Computer Club Analyzes Government Malware," *Chaos Computer Club*, https://ccc.de/en/updates/2011/staatstrojaner.

74 Herpig, 15-17.