R Street
Free markets. Real solutions.

R STREET POLICY STUDY NO. 237
July 2021

REFRAMING THE CRYPTO WARS

By Kathryn Waldron and Sofia Lesmes

INTRODUCTION

For the past several decades, policymakers, law enforcement, private companies, civil liberties advocates and cybersecurity specialists have been locked in a passionate yet seemingly unending battle over encryption. The debate, sometimes referred to as the "going dark problem" or the "crypto wars," centers around whether law enforcement agencies should be able to force companies to decrypt communications.[1] While advocates argue government access to encrypted data is necessary for the sake of public safety and national security, many others believe that undermining encryption is an assault on individual privacy and civil liberties. Despite decades of debate, policymakers and lawmakers have made minimal progress toward settling the issue once and for all or with finding an acceptable compromise.

CONTENTS

The debate was seemingly set to be answered by the courts in 2016, when Apple refused to craft new software at the behest of the Federal Bureau of Investigation (FBI) that would allow the agency to access encrypted information on a phone belonging to one of the shooters in a 2015 terrorist attack on Inland Regional Center in San Bernardino, California.

But the "going dark" encryption debate shares a key characteristic with the walking dead: no matter how many times you try to put it to rest, it keeps coming back. In October 2020, the Department of Justice (DOJ) issued an international statement calling for companies to "[e]nable law enforcement access to content in a readable and usable format where authorisation is lawfully issued, is necessary and proportionate, and is subject to strong safeguards and oversight."[2] Both at home and abroad, there are increased government calls to weaken encryption in the name of national security.

While fervor surrounding the issue remains high, trotting out the same arguments of a now decades-old policy debate has gotten us no closer to a solution. Indeed, several experts have agreed that if policymakers want to make progress, they must stop viewing encryption as an issue of security versus privacy and reframe the debate.

One laudable attempt to reframe how encryption policy is considered comes from Tim Maurer and Carnegie's working group on encryption, which brings together some of the premier experts on the topic.[3] While the working group does not come to a consensus regarding a policy solution, the

[1] See, e.g., John Mylan Taylor, "Shedding Light on the "Going Dark" Problem and the Encryption Debate," *University of Michigan Journal of Law Reform* 50:2 (2016). https://repository.law.umich.edu/mjlr/vol50/iss2/5; Bilgesu Sümer, "The rising tension in crypto wars: security through or despite encryption?" Ku Leuven Center for IT & IP Law, Nov. 24, 2020. https://www.law.kuleuven.be/citip/blog/the-rising-tension-in-crypto-wars-security-through-or-despite-encryption.

[2] Office of Public Affairs, "International Statement: End-to-End Encryption and Public Safety," Department of Justice, Oct. 11, 2020. https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety.

[3] Encryption Working Group, " Moving the Encryption Policy Conversation Forward," *Carnegie Endowment for International Peace*, Sept. 10, 2019. https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573.

group has proposed a number of recommendations for moving the conversation forward, such as narrowing the focus to encryption of data sitting in databases, known as data at rest, as opposed to data moving through a network, known as data in transit.[4]

The limiting binary of privacy versus security must be reshaped into one of security versus security, which focuses on coordinating a whole-of-government approach, creating a Bureau of Cyber Statistics, exploring alternatives and establishing a standard language to discuss encryption. However, there is still exploration to be done regarding why the privacy versus security framework has persisted for so long, and what additional steps must be taken to break away from this limiting way of thinking. The widespread availability of encryption and the highly public nature of certain cases where law enforcement has been stymied by technology, namely terrorist attacks, have obviously played their part in ensuring the debate remains relevant. However, also at play is the lack of a common language or good metrics and a reluctance on the part of certain government officials to explore potential alternative solutions.

A HIGHLIGHTS REEL OF THE U.S. ENCRYPTION DEBATE

At the heart of encryption lies the protection of the confidentiality, authenticity and integrity of data. Protecting data is often achieved through engineering confidentiality, or by preventing anyone besides the recipient from viewing the data in question. Protecting data can also mean ensuring that a certain individual sent a message, typically referred to as authentication. It can also mean determining that the message has not been tampered with in transit, known as integrity. To ensure authentication, integrity and confidentiality companies use algorithms to disguise data. Some of these systems use symmetric encryption, which uses the same key to encrypt and decrypt or asymmetric encryption, which uses different keys; many companies use a combination of both encryption types.

Hackers and government officials alike are often eager to access decrypted data, albeit for very different reasons. With ever increasing computing power, it is increasingly easy to crack protected data, and as a result, many companies are going to greater lengths to protect their data. Asymmetric cryptography—also known as public key cryptography—uses one-way mathematical functions to ensure confidentiality and authentication by using a recipient's public key to "lock" information, but only the recipient's private key can reveal the plaintext.[5] Conversely, a private key can encrypt a message, and a public key decrypts it, thus ensuring that a message was sent by the private key holder. Another method uses larger numbers as keys, and a third method works by storing the keys outside of a company database, which would almost certainly be targeted by malicious actors. However, these more rigorous types of encryption, generally known as strong encryption, are problematic for law enforcement as some companies design their software systems in such a way that they cannot decrypt certain data themselves to comply with subpoenas for information.

Below we will look at four key moments that have shaped and highlighted the development of the duality of security versus privacy including the creation of the Clipper chip, Edward Snowden's revelatory leaks of certain NSA and CIA programs, the 2016 San Bernardino terrorist attack and the 2020 EARN IT Act.

The Early "Crypto Wars" and the Clipper Chip

Perhaps the most formative event in the U.S. encryption debate's framing came in the 1990s, with the failed introduction of the Clipper chip, a microcircuit designed to enable the U.S. government and law enforcement to decrypt communications under warrant. The Clinton administration promoted the technology as a tool that struck a balance between privacy and security, ostensibly satisfying the dichotomy.[6] This argument based on fear that encryption would negatively impact law enforcement's ability to ensure public safety, came to dominate the encryption debate going forward, although the particular threat to public safety sometimes changes.

The chip's surveillance implications caused an immediate backlash from organizations including the Electronic Frontier Foundation (EFF) and Computer Professionals for Social Responsibility, the latter of which published a popular petition that received 50,000 signatures.[7] Coupled with the discovery of an existential vulnerability, the technology was obsolete by 1996.[8] Indeed, critics of the chip viewed it as part of a zero-game, a nearly existential threat to privacy in the name of national security.

[4] Tim Maurer, Arthur Nelson, "Out of the Political Trenches: Next Steps for Encryption Policy," *Carnegie Europe*, June 16, 2020. https://carnegieeurope.eu/strategiceurope/82081.

[5] Sam Metzler, "How does Public Key Encryption Work?" *Security Boulevard*, July 23, 2020. https://securityboulevard.com/2020/07/how-does-public-key-encryption-work.

[6] Office of the Press Secretary, "Statement by the Press Secretary," White House Archives, April 14, 1993. https://clintonwhitehouse6.archives.gov/1993/04/1993-04-16-press-release-on-clipper-chip-encryption-initiative.html.

[7] "Clipper Chip," *Computer Professionals for Social Responsibility*, October 1994. http://cpsr.org/prevsite/program/clipper/clipper.html.

[8] Parker Higgins, "On the Clipper Chip's Birthday, Looking Back on Decades of Key Escrow Failures," *Electronic Frontier Foundation*, April 16, 2015. https://www.eff.org/deeplinks/2015/04/clipper-chips-birthday-looking-back-22-years-key-escrow-failures.

The Encryption Debate Sequel: Snowden and Surveillance

Since the chip, the U.S. encryption debate has been peppered with similar events that, to a large extent, rehash the same arguments by pitting law enforcement supporters against privacy guardians. In 2013, intelligence contractor Edward Snowden decided to release swathes of highly sensitive and classified documents that revealed U.S. surveillance practices to journalists from a number of news outlets including The Washington Post and The Guardian.[9] Snowden's revelations caused controversy, indignation and shock worldwide, albeit for different reasons. While many individuals branded Snowden a traitor, others supported his legacy as a whistleblower.[10] Part of the reason for the range of reactions was the extent and capacity of government surveillance that was revealed by the released cache.

Besides debates about Snowden's legacy, his actions jump-started global privacy discussions in the digital age by ushering in a newfound sense of urgency. The "Snowden Effect," a term that encapsulates the shift in perspective around government data collection, also includes a turn toward encrypted communications to keep outsiders in the dark.[11] This shifted awareness highlights a core reason that people encrypt their communications: to ensure privacy. This development also highlighted that the privacy debate was not only important for those involved in illicit activities who needed to conceal themselves, but for anyone who used internet communications.[12] Through the shock that Snowden generated, the security versus privacy debate moved closer to mainstream discourse.

Privacy and the Encryption Debate

Two years later, the San Bernardino terrorist attack investigation evoked the most straightforward, high-profile battle of the binary encryption debate since the Clipper chip. After recovering one of the perpetrator's locked iPhones, the FBI was unable to bypass security controls for the investigation. A high-profile dispute ensued over whether or not Apple could be compelled to help the FBI access the iPhone's content by creating an intentionally vulnerable operating system. Ultimately, a third-party vendor unlocked the iPhone.

Although the issue was eventually settled out of court, the FBI-Apple lawsuit set off fierce debate about whether companies should undermine strong encryption practices for the sake of assisting law enforcement. Apple argued that creating a "GovOS" would create a slippery slope for data security on the whole.[13] Then Apple CEO Tim Cook asserted in a letter that, "this moment calls for public discussion, and we want our customers and people around the country to understand what is at stake."[14] Another critique surrounded the security of the intentionally vulnerable operating system. Experts agreed that the possibility of the OS falling into nefarious actors' hands was far from hypothetical and should be treated as a given. Public opinion, meanwhile, was nearly equally split on the issue.[15] A Pew Research Center poll found that 51 percent of surveyed thought that Apple should assist the FBI in unlocking the iPhone versus 38 percent who opposed it (11 percent who were unsure).[16]

Earn It: Encryption Controversy Over Section 230

In late 2020, the encryption debate was again revived, this time under the disguise of content moderation. A proposed amendment to Section 230 of the Communications Decency Act, referred to as the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act of 2020, provoked significant controversy among strong encryption advocates. Through an indirect mandate, law enforcement could be allowed to create backdoors into encrypted communications in the name of enforcement. While the bill's sponsor's argued that its focus was on stemming child sexual abuse material (CSAM) and not encryption, cybersecurity experts and privacy advocates pointed out that weakening encryption would not promote general public safety.[17] In addition, 26 organizations led by the Center for Democracy and Technology, including the R Street Institute, directed a letter to the sponsors of the EARN IT Act with a similar

[9] See, e.g., Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *The Washington Post*, June 7, 2013. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html; Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, June 6, 2013. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[10] See, e.g., PBS Newshour on YouTube, Jan. 24, 2014. https://www.youtube.com/watch?v=sQKUe96TAh4; Jonathan Topaz, "Kerry: Snowden a 'coward...traitor'," *Politico*, May 28, 2014. https://www.politico.com/story/2014/05/edward-snowden-coward-john-kerry-msnbc-interview-nsa-107157; "Edward Snowden is a Hero Not a Traitor," Amnesty International, last accessed July 14, 20021. https://www.amnesty.org/en/get-involved/take-action/Edward-Snowden-hero-not-traitor; Edward Snowden, (Root User), "Snowden: 'We Can Fix a Broken System'," *Electronic Frontier Foundation*, Dec. 26, 2020. https://www.eff.org/deeplinks/2020/12/we-can-fix-broken-system.

[11] Marcia Stepanek, "The Snowden Effect, and Opportunity?" *Stanford Social Innovation Review*, Aug. 8, 2013. https://ssir.org/articles/entry/the_snowden_effect_an_opportunity#.

[12] Tajdar Jawaid, "Privacy vs National Security," *International Journal of Computer Trends and Technology* 68:7 (July 2020), p. 5. https://arxiv.org/pdf/2007.12633.pdf.

[13] John Eden, "Why Apple is Right to Resist the FBI," *TechCrunch*, March 13, 2016. https://techcrunch.com/2016/03/13/why-apple-is-right-to-resist-the-fbi.

[14] "A Message to Our Customers," Apple, Feb. 26, 2016.https://www.apple.com/customer-letter.

[15] Brian Barrett, "The Apple-FBI Fight Isn't About Privacy vs. Security. Don't be Misled," *Wired*, Feb. 24, 2016. https://www.wired.com/2016/02/apple-fbi-privacy-security.

[16] "More Support for Justice Department Than for Apple in Dispute Over Unlocking iPhone," *Pew Research Center*, Feb. 22, 2016. https://www.pewresearch.org/politics/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone.

[17] Makena Kelly, "A Weakened Version of the EARN IT Act Advances Out of Committee," *The Verge*, July 2, 2020. https://www.theverge.com/2020/7/2/21311464/earn-it-act-section-230-child-abuse-imagery-facebook-youtube-lindsey-graham.

sentiment.[18] The controversy over the implications of the Act illustrates not just the tenacity of the encryption debate, but also its ability to seep into adjacent conversations.

The history of the U.S. encryption debate demonstrates that we have arrived at a security versus privacy binary through events that have further anchored themselves into discourse over time. Beyond the establishment of two camps, events show that each continues to use the same rhetoric with little results. In June 2020, the Lawful Access to Encrypted Data Act was introduced to try to circumvent past issues with encryption-related legislation. Despite these efforts, the proposal still resulted in an all-too familiar backlash.[19] Yet, a heated argument in the United States does not mean that we are the only country going through these growing pains with encryption.

THE CURRENT INTERNATIONAL DEBATE AROUND ENCRYPTION

Encryption has also become a topic of passionate debate outside of U.S. borders, with many countries struggling to reconcile the same priorities of public safety and privacy. Not surprisingly, countries with the most authoritarian political regimes have also embraced greater restrictions around encryption. For example, Russia amended a pre-existing counter-terrorism law in 2016 to create the commonly-named "Yarovaya Law." The Yarovaya law requires online services (which include special media networks or messaging services) to provide encryption keys to Russia's successor to the KGB, the Federal Security Service (FSB).[20] China has also passed legislation requiring internet firms and telecoms to assist the government with decrypting data, although China's law is not as invasive as its Russian counterpart.[21] Both of these laws were passed under the guise of counter-terrorism efforts.

However, U.S. allied countries have also found that the potential hindrance to counter-terrorism efforts remains a compelling argument, particularly in countries like France that have seen recent spates of terrorist attacks. In 2016, the legislation to mandate backdoors failed by only one vote.[22] During his 2017 presidential campaign, Emmanuel Macron called for "legal seizure of data from...encrypted services" and tweeted that "Internet players, if they persist in their position, will one day have to assume that they have been complicit in attacks."[23]

Former U.K. Prime Minister David Cameron has also flirted with the idea of backdoors into encrypted communications.[24] The United Kingdom also passed the Investigatory Powers Act in 2016, which allows cabinet ministers to order communication service providers develop the capacity to decrypt encrypted communications, although aspects of the Act's implementation remain unclear as the legislation has seen a slew of legal challenges.[25] Similar requirements have been legislated in Australia, with the passage of the 2018 Telecommunications and Other Legislation Amendment (Assistance and Access) Act (TOLA Act).[26]

Counter-terrorism is not the only argument gaining steam overseas. Brazil and India have both expressed concern about encryption hindering attempts to combat disinformation.[27] The governments of both countries have recently attempted to force American messaging service WhatsApp to violate the company's privacy protections. Disinformation, often spread via WhatsApp, has run rampant. Officials in Brazil are worried the spread of disinformation has influenced election results and discouraged people from receiving COVID-19 vaccinations.[28] WhatsApp is facing its own version of the 2016 Apple-FBI debate, as the company is currently embroiled in two legal cases where the Brazilian government says the company failed to obey judicial orders

[18] "Civil Society Coalition Condemns EARN IT Act for Threatening Free Expression, Encryption, and Child Abuse Prosecutions," *R Street Institute*, Sept. 16, 2020. https://www.rstreet.org/2020/09/16/civil-society-coalition-condemns-earn-it-act-for-threatening-free-expression-encryption-and-child-abuse-prosecutions.

[19] See, e.g., Jillian Foley, "A Republican Bill Would Weaken Encryption Just When We Need It Most," *Slate*, June 29, 2020. https://slate.com/technology/2020/06/lawful-access-encrypted-data-act.html; Andrew Crocker, "The Senate's New Anti-Encryption Bill Is Even Worse Than EARN IT, and That's Saying Something," *Electronic Frontier Foundation*, June 24, 2020. https://www.eff.org/deeplinks/2020/06/senates-new-anti-encryption-bill-even-worse-earn-it-and-thats-saying-something.

[20] Danny O'Brien and Eva Galperin, "Russia Asks For The Impossible With Its New Surveillance Laws," *Electronic Frontier Foundation*, July 19, 2016. https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws.

[21] Scott J. Shackelford, et al. "Decrypting the Global Encryption Debate," *Harvard Belfer Center*. https://www.belfercenter.org/publication/decrypting-global-encryption-debate.

[22] Ross Schulman and Kevin Bankston, "Deciphering the European Encryption Debate: France," *New America*, July 31, 2017. https://www.newamerica.org/oti/policy-papers/deciphering-european-encryption-debate-france.

[23] Emmanuel Macron (@EmmanuelMacron), "Les acteurs de l'Internet, s'ils persistent dans leur position, devront assumer un jour d'avoir été complices d'attentats. #LutteTerrorisme," April 10, 2017, 6:25AM, Tweet. https://twitter.com/EmmanuelMacron/status/851380639261765632.

[24] Jane Wakefield, "Can the government ban encryption?" *BBC*, Jan. 13, 2015. https://www.bbc.com/news/technology-30794953.

[25] Natasha Lomas, "Liberty's Challenge to UK state surveillance powers reveals shocking failure," *TechCrunch*, June 11, 2019. https://techcrunch.com/2019/06/11/libertys-challenge-to-uk-state-surveillance-powers-reveals-shocking-failures.

[26] Stilgherrian, "The Encryption Debate in Australia: 2021 Update," *Carnegie Endowment for International Peace*, March 31, 2021. https://carnegieendowment.org/2021/03/31/encryption-debate-in-australia-2021-update-pub-84237.

[27] Richard Wingfield, "Trends In The Encryption Debate: From Intelligence Gathering To Tackling Online Harms," *Global Partners Digital*, Jan. 18, 2021. https://www.gp-digital.org/trends-in-the-encryption-debate-from-intelligence-gathering-to-tackling-online-harms.

[28] See, e.g., "The Misinformation Bubble Threatening Brazil's Indigenous People," *BBC News*, May 8, 2021. https://www.bbc.com/news/blogs-trending-56919424; Daniel Avelar, "WhatsApp fake news during Brazil election 'favoured Bolsonaro'," *The Guardian*, Oct. 30, 2019. https://www.theguardian.com/world/2019/oct/30/whatsapp-fake-news-brazil-election-favoured-jair-bolsonaro-analysis-suggests.

to hand over decrypted data.[29] A similar lawsuit is unfolding in India, where in May 2021 Facebook and WhatsApp both challenged a new Indian law that attempted to instill "traceability" requirements that would undermine the companies' encryption practices.[30] Both cases have yet to reach a legal conclusion.

The Impact of International Encryption Policy on Domestic Policy

It is important to pay attention to these global debates, as the international community's general commitment for or against strong encryption could no doubt have a ripple effect on U.S. policy. A 2018 study from the Hoover Institute details many of the trans-national effects caused by previous policy actions, noting the numerous pathways through which both government and private sector policies create impact. In general, these ripple effects are stronger in cases where the government or private sector is located in a country with an outsized impact on the global economy or international norms setting, such as the United States and China. For example, Snowden's reveal of NSA surveillance operations contributed to decreased sales for many American companies, with an estimated $35 billion to $180 billion in lost revenue.[31]

U.S.-based companies and policymakers would need to consider how any legal ban on strong encryption will interact with other countries' legislation. This issue was touched on by the European Commission, who considered how this might impact the EU's General Data Protection Regulation (GDPR).

> Should the U.S. enact new legislation in this area, the Commission will carefully assess its impact on the adequacy finding for the EU-U.S. . . . A downgrading of the EU-U.S. Privacy Shield hinted at in this answer would likely prove very disruptive to U.S.-based business on the Internet. Without an adequacy finding, each company seeking to do business involving cross-border data would have to implement additional and burdensome compliance practices.[32]

Finally, it must also be acknowledged that one of the biggest barriers to any domestic legislation weakening encryption is the global availability of non-compliant products. Customers concerned about Apple handing over private messages could easily switch to messaging apps from non-U.S. companies or even globally distributed, open-source platforms, such as Telegram. Law enforcement would be no better off than they are now and American companies would lose their competitive advantage in the global marketplace.

SECURITY VERSUS PRIVACY OR SECURITY VERSUS SECURITY

As noted above, the most common arguments in favor of government access to encrypted data, both inside and outside the United States, all center around some form of protecting public safety, either regarding stopping terrorism, preventing the spread of child sexual abuse materials or tracing the spread of disinformation. On the other side of the debate are privacy advocates. Indeed, a security versus privacy perspective is traditionally how people have perceived the two sides of the encryption debate.

However, security versus privacy is a problematic framework that is becoming increasingly weak as the number of cybersecurity threats we face grow larger. American cryptographer Bruce Schneier points out a number of data thefts made possible by weakened or non-existent encryption practices, and stated that the security versus privacy debate offers only

> a myopic framing that focuses only on one threat—criminals, including domestic terrorists—and the demands of law enforcement and national intelligence. This obscures the most important aspects of the encryption issue: the security it provides against a much wider variety of threats.[33]

Several other experts have also argued that the encryption debate would be more accurate if framed under the guise of security versus security, as opposed to security versus privacy, and that the national security benefits of allowing strong encryption outweigh the difficulties posed to law enforcement. For example, many Washington politicians and policymakers discuss important information over personal devices, which is a problem that was magnified in 2018 when it was revealed that Russia and China were listening in to calls made by former President Trump. As Susan Landau and Steven Bellovin noted in their response to the situation at *Lawfare*:

> if instead of the U.S. government fighting the spread of strong cryptography, the National Security Agency

[29] Priscilla Silva et al., "The Encryption Debate in Brazil: 2021 Update," *Carnegie Endowment for International Peace*, March 31, 2021. https://carnegieendowment.org/2021/03/31/encryption-debate-in-brazil-2021-update-pub-84238.

[30] Aditya Kalra and Sankalp Phartiyal, "Indian Government Exceeded Powers With Encryption-breaking Rule - WhatsApp Filing," *Reuters*, May 26, 2021. https://www.reuters.com/technology/indian-government-exceeded-powers-with-encryption-breaking-rule-whatsapp-filing-2021-05-26.

[31] Budish, Ryan, Herbert Burkert, and Urs Gasser. "Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects." *Hoover Institution*, 2018. https://dash.harvard.edu/bitstream/handle/1/36291726/budish_webreadypdf%202.pdf?sequence=1&isAllowed=.

[32] Jenny L. Holmes, Vincent J. Tennant, "U.S. Encryption Debate Sparks Questions at the European Commission," *Nixon Peabody*, Dec. 18, 2019. https://www.nixonpeabody.com/en/ideas/blog/data-privacy/2019/12/18/u-s-encryption-debate-sparks-questions-at-the-european-commission.

[33] Bruce Schneier, "Security or Surveillance?" *Lawfare*, Feb. 1, 2016. https://www.lawfareblog.com/security-or-surveillance.

> and FBI had pushed for cellphones that would always encrypt communications end-to-end . . .It would also mean that every legislator and legislative aide, every chief executive, every financial officer—indeed, any person who had information that would be useful to an eavesdropper, whether it be China, Russia, an industrial competitor or a criminal organization—would necessarily use phones that routinely secured their conversations.[34]

The persistence of the security versus privacy framework is problematic for several reasons. First, because as noted above, it is so superficial as to be untrue. It allows law enforcement and privacy advocates to talk past one another, each focused on the merits of their own cause. It also implies that privacy and security are inherently locked in a tradeoff, so that to have one necessitates forgoing the other. But this is not the case, either. Weakening encryption may assist law enforcement with pursuing certain bad actors, but it will also open our networks and our devices to a panoply of new adversaries. That can hardly be called true security.

It is our hope that reframing the debate will breathe new life into this issue, requiring policymakers and industry alike to consider their own stances and biases and look for new and creative solutions.

CHALLENGES TO MAKING PROGRESS IN THE ENCRYPTION DEBATE

There are a number of factors that have prevented the security versus privacy aspect of the encryption debate from being put to rest, and that hinder both sides from coming to a consensus.

The Increased Availability of User-friendly Encryption Services

One of the foremost reasons the encryption debate remains evergreen is that as a society, we are constantly facing a number of threats involving encrypted data. The threats themselves are not new—terrorism, child pornography, and even the weaponization of information and propaganda existed before the internet and will continue to be problems if encryption were to suddenly disappear. However, it is true that malicious actors have taken advantage of encryption technology. Law enforcement and others on the anti-strong encryption side are correct that encryption technology significantly complicates their jobs.

That does not mean backdoors and other ways to weaken encryption are worth the additional security risks they would bring. With the benefit of a backdrop of rising skepticism of big tech's capacity to be a good steward of information, the increase of recent tech-assisted attacks have given the DOJ a gamut of examples to point to when arguing for government access to encrypted data.[35] While experts have pointed out that mandating backdoors and golden keys are unlikely to actually hinder terrorists, the fear caused by terrorist attacks continues to fuel many of the pro-government access side's talking points.[36]

Of course, it is worth noting that politically charged events need not necessarily lead to increased support for government access to encrypted data. For example, increased societal concern about police brutality against black Americans and the rise of Black Lives Matter (BLM) has generally decreased public support for law enforcement, also dampening any support for granting said law enforcement additional surveillance capabilities. Several members of the BLM movement spoke out on behalf of Apple during the company's legal battle with the FBI. A letter from civil rights activist Rev. Jesse Jackson to the judge overseeing the case expressed the movement's concerns, stating, "If the government prevails against Apple, it is my fear that it will accelerate—and make easier—government efforts to 'hack' into the legitimate activities of civil rights organizations."[37]

End-to-end encrypted messaging services are often relied upon by the champions of social justice, as seen recently by protestors in both the United States and Hong Kong.[38] Positive public perceptions of movements like Black Lives Matter or other protesters, unlike the 2015 terrorist attack on San Bernardino's Inland Regional Center, might well discourage any sort of government crackdown on encryption technologies due to concern about raising public ire.

A Lack of a Common Language

Another challenge any successful reframing of the debate will need to address is the fact that each stakeholder in the encryption debate—technologists, law enforcement, civil rights activists and policymakers alike—all speak a different language with its own unique jargon. It is not always easy to

[34] Steven M. Bellovin, Susan Landau, "Encryption by Default Equals National Security," *Lawfare*, Oct. 26, 2018. https://www.lawfareblog.com/encryption-default-equals-national-security.

[35] Megan Brennan, "Views of Big Tech Worsen; Public Wants More Regulation," *Gallup*, Feb. 18, 2021. https://news.gallup.com/poll/329666/views-big-tech-worsen-public-wants-regulation.aspx.

[36] Aaron Brantly, "Banning Encryption to Stop Terrorists," *CTC Sentinel* 10:7, (August 2017). https://ctc.usma.edu/banning-encryption-to-stop-terrorists-a-worse-than-futile-exercise.

[37] Cory Bennett, "Black Lives Matter Gets Behind Apple in Encryption Fight," *The Hill*, March 17, 2016. https://thehill.com/policy/cybersecurity/273348-black-lives-matter-gets-behind-apple.

[38] Amelia Nierenberg, "Signal Downloads Are Way Up Since the Protests Began," *New York Times*, June 11, 2020. https://www.nytimes.com/2020/06/11/style/signal-messaging-app-encryption-protests.html.

"translate" between these different sets of jargon, however, the likelihood of talking past one another only hinders progress in coming to agreement. As one scholarly paper puts it:

The best way to resolve the ambiguity of such a complex concept as "cybersecurity",

> along with some other encryption-related concepts (e.g. backdoor, phishing, etc.), is to ensure effective communication among different research communities to further objectives and to contribute to meaningful dialogue between professionals and policy-makers. However, there is still little consensus on the meaning of "cybersecurity" and "cyberspace", despite attempts to develop common vocabularies.[39]

Similarly, a study of the term "backdoor" and the rhetoric and metaphors typically accompanying the term, concludes:

> Since we do not seem to have made considerable progress in combating the ever-growing range of information security threats, the further search for apt analogies is highly critical both for policy-makers and IT experts community to adequately structure the IT discourse.[40]

It is worth noting that opinions of issues reliant on technical terms that have additional meaning outside of cybersecurity (like backdoor or virus), will not only be dependent on the individual's knowledge of the jargon in question, but will also be influenced by any connotation with the more commonly understood meaning of the term.

The term backdoor exemplifies the role of rhetoric in blurring perceptions. As the study points out, the word backdoor is used by the IT community to describe both licit portals used by system administrators to troubleshoot problems and illicit portals used by bad actors for malicious purposes.[41] The term similarly has a dual meaning outside of cybersecurity, as backdoors can literally be used for entrance to a building for both lawful and unlawful purposes.

The rhetorical techniques used by both sides of the encryption debate may be useful in drawing sympathy for their own side, but they are not useful for coming to a policy solution.[42] If we want to see progress on the encryption debate then we need to ensure everyone is speaking the same language. One way to do this is to stop using overly broad arguments when it comes to encryption and to avoid conflating distinct issues as though any problems related to access to data are interchangeable. As Matt Tait argues, the confusion that comes from government officials "bundling" different scenarios involving different types of encryption methods into a broader debate actually hinders conversation.

> each category poses very different challenges to investigations, provides dissimilar security benefits to users, and has surprisingly unrelated options, alternatives and trade-offs for any proposed path forward for law enforcement or technology companies to adapt to their respective challenges.[43]

However, a common vocabulary alone is not sufficient for creating a robust cross-sectional dialogue. Equally necessary is a common pool of evidence and metrics. Otherwise we are making policy in the dark, attempting to weigh theoretical possibilities and guessing which side of the scale is lower. If law enforcement is worried that strong encryption prevents them from catching child sexual predators, then we need statistics regarding the number of cases not solved each year due to strong encryption. Likewise, we need better metrics regarding the cybersecurity threats our nation faces. As noted in R Street's bibliography of cyber metrics, while some qualitative measurements of cybersecurity exist, we still lack accurate quantitative methods of assessing cybersecurity. [44] The Biden administration's creation of a Cybersecurity Safety Review Board looks to be a step in the right direction, but there is still plenty of information regarding our cyber posture that we do not really know.[45]

A Lack of a Whole of Government Approach to Cybersecurity

Although the encryption debate is sometimes depicted as big tech versus big government, this portrayal is so shallow as to be inaccurate. In nearly all countries, the government includes both proponents and opponents of strong encryption. Even in countries with authoritarian governments, like Russia and China, the passage of encryption-oriented

[39] Inna Skrynnikova, "Metaphor Co-Creation in Reframing Cybersecurity Issues," *RAEL- Revista Electrónica de Lingüística Aplicad* 19:1, (November 2017). https://rael.aesla.org.es/index.php/RAEL/article/view/377.

[40] Inna Skrynnikova, "Analogical reasoning in uncovering the meaning of digital-technology terms: the case of backdoor," *Journal of Computer-Assisted Linguistic Research* 4, May 22, 2020, pp. 23-46. https://riunet.upv.es/bitstream/handle/10251/144775/Skrynnikova%20-%20Analogical%20reasoning%20in%20uncovering%20the%20meaning%20of%20digital-technology%20terms:%20the%20cas....pdf?sequence=1.

[41] Ibid.

[42] Herb Lin, "The Rhetoric of the Encryption Debate," *Lawfare*, Oct. 12, 2015. https://www.lawfareblog.com/rhetoric-encryption-debate.

[43] Matt Tait, "Decrypting the Going Dark Debate," *Lawfare*, Oct.17, 2017. https://www.lawfareblog.com/decrypting-going-dark-debate.

[44] Kathryn Waldron, "Resources for Measuring Cybersecurity," *R Street Institute*, Oct. 29, 2019, p. 4. https://www.rstreet.org/2019/10/29/resources-for-measuring-cybersecurity.

[45] Jonathan Greig, "An NTSB for cyber attacks? Critics grapple with Biden's Cybersecurity Safety Review Board plan," *ZDNet*, May 24, 2021. https://www.zdnet.com/article/congressional-leaders-experts-debate-viability-of-cybersecurity-safety-review-board-described-in-biden-executive-order.

legislation has prompted heated disagreement among politicians and government officials. For example, the security firm Kaspersky has focused on distancing itself from its Russian origins and has moved some of its core operations to Switzerland.[46]

In the United States and Europe, the disagreement has been even more intense and divisive. While the U.S. Department of Justice, and particularly former Attorney General Bill Barr, have been among the most outspoken advocates for the creation of backdoors, Rohit Chopra was equally vocal in his support for strong encryption during his time as Federal Trade Commissioner. Similarly, the ultimate lack of Congressional action on the issue is not surprising given the range of policy stances that have cropped up in proposed legislation.

Encryption is a complex issue that encapsulates many competing values, and there is merit in seeing that all of these values have their own champions within our government. However, the lack of a whole of government approach to strong encryption, and to American cybersecurity in general, is troubling given the increasing number of attacks we've seen on the security of our networks. Having the DOJ and the FBI call for backdoors and golden keys does not instill faith that the government views protecting the security of American networks as a priority. In his piece *Rethinking Encryption*, former RSI colleague Jim Baker, who worked for the FBI during the San Bernardino case, argues,

> federal, state and local governments should be doing everything they can to enhance the cybersecurity status of the nation. All public safety officials should think of protecting the cybersecurity of the United States as an essential part of their core mission to protect the American people and uphold the Constitution. And they should be doing so even if there will be real and painful costs associated with such a cybersecurity-forward orientation.[47]

However, one concern in adopting a whole-of-government approach to encryption is that the Biden administration should learn the importance of transparency from its predecessors' approach to the Vulnerabilities Equities Process (VEP). Although VEP, the process used by the federal government to determine whether or not to disclose any discovered zero-day vulnerabilities, first began in 2008, public knowledge was extremely limited until 2016 after the Electronic Frontier Foundation submitted a FOIA request.[48] The secretive nature of the program has only bred public distrust, particularly from private companies whose vulnerabilities were not reported. Encryption, like vulnerability disclosure, requires a cohesive, holistic approach, but if the government is not transparent they might end up fanning the flames of controversy instead.

Disagreement About Backdoor Alternatives

Perhaps the most frustrating challenge is the government's lack of enthusiasm about publicly exploring practical alternatives to backdoors. One alternative which has recently been proposed, particularly to address concerns related to CSAM, is client-side scanning CSS. With CSS, messages or files would be scanned by software before being encrypted and sent on its merry way. Any message or file that was flagged as containing illicit materials could then be flagged and intercepted in an intelligible state. However, CSS also faces significant challenges. For example, the scanning would only be efficient if the software algorithm used was accurate. Too many false negatives would leave law enforcement no better off than they are now, while too many false positives would lead to significant privacy violations. A more detailed review of the potential problems with CSS can be found in Paul Rosenzweig's piece "The Law and Policy of Client-Side Scanning" in *Lawfare*.[49]

A more currently viable alternative is lawful hacking, which has been used more extensively in other countries like Germany. In this case, instead of requiring companies to purposefully weaken their own security practices, law enforcement works with a third-party to legally hack into a device.

Of course, lawful hacking comes with its own challenges that would need to be addressed. One challenge is whether law enforcement or involved third parties should be required to disclose security vulnerabilities discovered in the process of hacking into a device. As many have pointed out in regards to the NSA, the government has an incentive not to reveal these weaknesses so they can exploit them in future investigations. However, willfully hiding these findings leaves people vulnerable to malicious actors who may also discover and exploit the hole in the company's cybersecurity.[50]

Another concern is that sanctioning the U.S. government to lawfully hack devices legitimizes the practice by other

[46] "Kaspersky completes its data-processing relocation to Switzerland and opens new Transparency Center in North America," *Kaspersky*, Nov. 17, 2020. https://www.kaspersky.com/about/press-releases/2020_kaspersky-completes-its-data-processing-relocation-to-switzerland-and-opens-new-transparency-center-in-north-america.

[47] Jim Baker, "Rethinking Encryption," *Lawfare*, Oct. 22, 2019. https://www.lawfareblog.com/rethinking-encryption.

[48] Andi Wilson Thompson, "Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter," *Lawfare*, Jan.13, 2021. https://www.lawfareblog.com/assessing-vulnerabilities-equities-process-three-years-after-vep-charter.

[49] Paul Rosenzweig, "The Law and Policy of Client-Side Scanning," *Lawfare*, Aug. 20, 2020. https://www.lawfareblog.com/law-and-policy-client-side-scanning.

[50] Carlos Liguori, "Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate," *Michigan Technology Law Review* 26:2 (2020), pp. 330-334. https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1019&context=mtlr.

nation-states who may lack adequate due process protections. And while due process in the U.S. is certainly more rigorous than many countries, we currently lack a strong regulatory framework that would determine which authorities should have access to what data and when. As Marshall Erwin points out,

> lawful hacking capabilities might be more likely to be abused than more traditional law enforcement tools…. because, even if we establish the appropriate legal standards to govern this activity, there will almost certainly be fewer external checks to ensure those standards are met.[51]

A third challenge is the risk of incidental additional privacy violations, as data not included in a warrant could become accessible in the process of hacking. Of course, not all law enforcement bodies have equal access to the necessary resources. While the DOJ and FBI are well-resourced, local law enforcement in a region with few tech firms are far less likely to have the capabilities needed to break into a device. Finally, lawful hacking is time-consuming and, for the government at least, costlier than building in backdoors. As a result, some government officials, such as Former FBI Director James Comey, have stated that they do not view lawful hacking as sufficient.[52]

Lawful hacking may not be a perfect solution but it is generally agreed to be better for protecting cybersecurity than building backdoors. Instead of holding out for their dream solution, government officials should embrace lawful hacking and promote the creation of a good regulatory regime that can instill the necessary safeguards to determine when and how lawful hacking should occur. As Kevin Bankston has argued,

> as unbreakable encryption proliferates, so too will government hacking necessarily increase, whether advocates like it or not. Therefore there's little to lose and much to gain if Congress affirmatively regulates when and how the government gets to hack, along with when and how it gets to keep software vulnerabilities secret instead of disclosing them.[53]

Still, the FBI and DOJ should acknowledge that both organizations have still managed to conduct a number of successful operations, despite lack of access to encrypted communications, including retrieval of the Colonial Pipeline ransom. Even more impressive was "Trojan Shield," an operation that led to the arrest of approximately 800 criminals who were caught through an encrypted messaging app actually built by the FBI.[54] When the government stops fighting encryption and starts putting its effort into improving its existing tools, they are more successful.

CONCLUSION

From the early Crypto Wars to similar debates today, the encryption debate has moved slowly. This is due to factors including a lack of cohesive language, an unsteady hand from government actors throughout the decades, and events that happen as a result of unresolved questions. To move forward, these stakeholders must stop asking the same questions and instead be cognizant of what has inhibited progress so far. Terminology and framing are two factors that require attention. If these factors are considered, perhaps we can avoid yet another scenario like the 2020 Lawful Access to Encrypted Data Act, which one senator claimed "puts a wig and a mustache on the same tired argument that pro-surveillance activists have been making since the 1990s."[55]

There are some key next steps that will address the challenges mentioned above.

1. The White House should charge incoming National Cyber Directors with developing a whole-of-government encryption policy. As part of this approach, the NCD should choose to prioritize our nation's cybersecurity, perhaps developing an American version of Germany's five "crypto principles."[56]

2. The White House and Congress should also establish a Bureau of Cyber Statistics that can gather data and develop metrics regarding encryption so we have a better understanding of the number and types of attacks deterred by strong encryption and the number of law enforcement cases actually stymied by lack of access to encrypted data.

3. While neither CSS nor lawful hacking are perfect alternatives, the DOJ and FBI should more publicly embrace creative ways to bypass the need for back-

[51] Marshall Erwin, "Lawful Hacking After the Encryption Debate," *Just Security*, Oct. 15, 2015. https://www.justsecurity.org/26849/lawful-hacking-encryption-debate.

[52] Daniel Zhang, "Revisit The Case for Lawful Hacking: A Path to the Going Dark Debate," *Georgetown Security Studies Review*, Dec. 13, 2019. https://georgetownsecuritystudiesreview.org/2019/12/13/revisit-the-case-for-lawful-hacking-a-path-to-the-going-dark-debate/#_edn23.

[53] Kevin Bankston, "Ending The Endless Crypto Debate: Three Things We Should Be Arguing About Instead of Encryption Backdoors," *Lawfare*, June 14, 2017. https://www.lawfareblog.com/ending-endless-crypto-debate-three-things-we-should-be-arguing-about-instead-encryption-backdoors.

[54] Joseph Marks, "The Cybersecurity 202: The Justice Department is racking up wins despite encryption concerns," *Washington Post*, June 16, 2021. https://www.washingtonpost.com/politics/2021/06/16/cybersecurity-202-justice-department-is-racking-up-wins-despite-encryption-concerns.

[55] Cyrus Farivar and Kevin Collier, "‹Lawful access› bill would allow feds to legally bust into encrypted devices," *NBC News*, June 24, 2020. https://www.nbcnews.com/tech/security/lawful-access-bill-would-allow-feds-legally-bust-encrypted-devices-n1232071.

[56] Sven Herpig, Stefan Heumann, "The Encryption Debate in Germany," *Carnegie Endowment for International Peace*, May 30, 2019. https://carnegieendowment.org/2019/05/30/encryption-debate-in-germany-pub-79215.

doors. Additionally, Congress should begin preemptively building a regulatory framework for lawful hacking to clarify use and prevent abuse by updating the Computer Fraud and Abuse Act.

4. Policymakers and experts alike should strive to discuss the encryption debate in more concrete terms instead of resorting to broad generalizations. Furthermore, the White House should assign the Dept. of Commerce with coordinating and convening both public and private stakeholders to establish an agreed-upon common lexicon.

If we want to make progress on the encryption debate, we all need to talk the same language and we need to recognize the folly of pitting privacy against security. While the above recommendations will not solve all of the problems raised by the encryption debate, we believe they would mitigate some of the challenges and help clear the debris from the path moving forward.

ABOUT THE AUTHORS

Kathryn Waldron is a fellow with R Street's Cybersecurity and Emerging Threats team. Her work focuses on the intersection of economics, geopolitics and cybersecurity.

Sofia Lesmes is a research associate with R Street's Cybersecurity and Emerging Threats team. She focuses on data security and data privacy.