accessnow

accessnow.org

Encryption in the U.S.: Crypto Colloquium Outcomes Report

January 2018

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

Abstract

U.S. government agencies have identified the inability to access information on encrypted mobile phones as one of the largest current challenges to criminal investigations. In September 2017, Access Now, supported by the Mozilla Foundation's Tech Policy Fellowship, hosted the Crypto Colloquium — an invite-only dialogue, with participation under the Chatham House rules — to discuss this challenge. Participants represented four stakeholder groups: civil society, academic experts, technology companies, and former U.S. government officials.

The discussion began with the assumption that it is technically possible to build mechanisms that allow law enforcement and intelligence agencies access to the material on encrypted devices without the user's assistance.

The Crypto Colloquium was a discussion of the legal, security, and economic consequences of mandating this type of mechanism in order to ensure government access to content information on devices. The conversations overlapped in several meaningful ways, producing important observations that the participants largely agreed upon, although not necessarily unanimously.

In this report we provide a summary of the lessons learned, as well as some more general "unanswered questions" that participants identified as needing more research and analysis. The report begins with a history of the debate over encryption and description of the methodology for the Crypto Colloquium.

Table of Contents

Introduction and Background

The Crypto Colloquium took place on September 25, 2017 in Washington, DC. It was a closed-door event that included technologists, members of civil society, company representatives, and former government officials, who met to discuss the issue of encryption. The discussion began with the assumption that it is technically possible to build mechanisms that allow law enforcement and intelligence agencies access to the material on encrypted devices without the user's assistance. With this in mind, participants were asked to identify impacts that such mechanisms would have, particularly on three areas: law, security, and the economy.

The one-day conversation was the third event of a series, building on and furthering the outcomes of two previous events: Crypto Summit 1.0 and Crypto Summit 2.0. The Crypto Colloquium used the outcome documents from both the first and second Crypto Summits as the basis for the conversation, along with two other keystone reports: "Don't Panic: Making Progress on the Going Dark Debate,"[1] a 2016 report by the Berkman Klein Center for Internet & Society signed by 12 experts in law, policy, and technology, and "Exploring Encryption and Potential Mechanisms for Authorized Government Access to Plaintext,"[2] an outcome document of a workshop hosted by the National Academies of Sciences, Engineering, and Medicine.

Crypto Summit 1.0 was a daylong series of sessions about cryptography.[3] Speakers included crypto war veterans, academics, corporate and government representatives, technologists, experts, and ordinary internet users.[4] The first session discussed the modern history of the debate around encryption, followed by a mapping of the encryption ecosystem. In a third session, legal experts discussed the law as applied to encryption. All three of these initial sessions were punctuated by a series of short, lightning-style presentations about the use of encryption. The event led up to a fourth session, which identified the challenges and opportunities provided by encryption. These included:

CHALLENGES

1. Encryption is often not usable, functional, or dependable;
2. Criminals are often eager to adopt encryption;
3. The legal environment surrounding encryption is opaque;
4. Complex systems, both technical and social, are difficult to develop;
5. There is an essential tension between lawful surveillance and privacy; and
6. Many methods of encrypting communication do not protect metadata.

OPPORTUNITIES

1. Developing technology that makes encryption easy, effective, and ubiquitous;
2. Creating a culture that values secure communication;
3. Increasing user control over information;
4. Protecting the integrity and confidentiality of information against state and non-state actors;
5. Enhancing user trust in the businesses that control the means of communication;
6. Increasing competitive advantage for privacy-enhancing tool makers; and
7. Defeating overbroad surveillance by having tools and platforms encrypt by default.

[1] https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[2] https://www.nap.edu/read/23593/chapter/1.

[3] https://www.accessnow.org/crypto_summit_part1/.

[4] https://s3.amazonaws.com/access.3cdn.net/0cd9a20a53838aab7f_0cwm680ei.pdf.

Crypto Summit 2.0, which took place alongside RightsCon Silicon Valley in 2016,[5] consisted of a series of simultaneous workshops.[6] These workshops examined umbrella issues identified at the first event, and were designed to provide a forum to directly analyze key questions surrounding the use of cryptography and government access, examine concrete outcomes, and identify areas for future work and discussion. Among other things, the leaders of the tracks facilitated conversations that produced a series of factors to consider when examining techniques to access encrypted data,[7] ways to measure economic cost of any mandated methods for obtaining that access,[8] and a list of projects that could help expand access to encryption to those who most need it.[9]

This Crypto Colloquium was supported by Access Now and the Mozilla Foundation's Tech Policy Fellowship. We would like to thank everyone who participated for their contributions, including Kevin Bankston (New America's Open Technology Institute), Alan Davidson, Benjamin Dean (Center for Democracy and Technology), Sharon Bradford Franklin (Georgetown Center on National Security and the Law), Barry Friedman (Policing Project at NYU Law School), Anne Hobson, Chris Riley (Mozilla), and Julian Sanchez. Access Now would also like to thank the Internet Association for its generous support of this event.

[5] https://www.rightscon.org/rightscon-silicon-valley-2016-videos/.

[6] https://www.accessnow.org/crypto-summit-2-0/.

[7] https://www.accessnow.org/cms/assets/uploads/2016/07/CS2.0_Outcomes_Track1.pdf.

[8] https://www.accessnow.org/cms/assets/uploads/2016/07/CS2.0_Outcomes_Track2.pdf.

[9] https://www.accessnow.org/cms/assets/uploads/2016/07/CS2.0_Outcomes_Track4.pdf.

[10] https://www.youtube.com/watch?v=AUOfpIPztKM.

[11] https://www.senate.gov/artandhistory/history/resources/pdf/aaron_burr.pdf.

[12] http://www.history.com/news/aaron-burrs-notorious-treason-case.

[13] http://www.famous-trials.com/burr/162-letter.

[14] http://volokh.com/posts/1198712224.shtml.

History of the Encryption Fight

In the United States, the discussion over the development and use of encryption systems is almost as old as the country itself.

Thanks to Lin-Manuel Miranda and the success of *Hamilton*, some of the finer points of the hotly contested election between Aaron Burr and Thomas Jefferson to be the third President of the United States are now widely known.[10] Burr served as Jefferson's vice-president during his first term, from 1801-1805.[11] Only two years later, Burr would be brought to trial for treason, having been accused of a vast conspiracy, many of the details of which have been lost to history.[12] At the heart of the trial was a letter written in code from Burr to General James Wilkinson.[13] Burr's secretary, known only as Willie, was called to testify, and was asked whether he could read the letter (that is, if he knew the key), which would have tied it back to Burr. Willie invoked his Fifth Amendment right against self-incrimination, but this was overcome; essentially, knowing the cipher did not implicate him in the contents thereof.[14]

Notably, at the time, there was no question about whether one could use encryption; only how, once written, a court would deal with the cipher. Breaking codes was not the key problem because they could generally be cracked. This was true all the way through World War II, when William and Elizabeth Friedman helped to coin the term "cryptanalysis" to describe the art of codebreaking. However, modern computing has now introduced new complexities and exponentially increased the power of encryption. Today it is nearly impossible to forcibly decrypt a digitally encoded message. Instead, codebreakers rely on other methods: they exploit vulnerabilities in the encryption system; gain access to the message before it has been encrypted or after decryption; or acquire encryption keys.

Modern technology has also virtually erased the distinction between encryption systems used by government targets and those used by everyone else. This means that when the government wants to gain access to the digital communications of a target, the authorities are likely poking through the same encryption schemes that protect your private information when, for example, you send your credit card information to a retailer or share a personal photograph with a loved one.

The various means used to break modern encryption have been at the center of a policy debate dating back to the establishment of "export controls" in the 1970s used to limit the strength of encryption that could be distributed outside the United States. The majority of these export controls have been removed today, though some remain. In the 1990s a series of proposals focused on a concept known as "key escrow" and a piece of technology known as the "Clipper Chip." Key escrow is a system by which encryption keys used to protect communications are stored by a third party, typically either a government or private sector entity. The Clipper Chip is an encryption device the U.S. government wanted to mandate the use of, employing a key escrow system to ensure available access.[15] The proposal was already under heavy criticism when the discovery of vulnerabilities in the Clipper Chip finally sunk it. The debates over this system formed the basis for what are known as "the Crypto Wars," now sometimes called "Crypto Wars 1.0."

In nearly two decades following the death of the Clipper Chip and the removal of most export controls, encryption spread widely and became a cornerstone for secure electronic commerce. But during this time, representatives of the U.S. government, primarily at the Federal Bureau of Investigation (FBI), raised the issue of encryption from time to time, claiming that they were "going dark," meaning that they were losing access to information and communications that would otherwise be available in relation to operations and investigations. Statistics were floated about how encryption impacted law enforcement, but serious questions have been raised about whether these numbers are a reliable estimate of how encryption acts as a barrier. Further, experts speculate that rather than "going dark," law enforcement has benefited from the vast increase in information easily available in the digital age, including not only metadata but also content records stored with third parties that would otherwise have been kept in private residences, business filing cabinets, or other secure facilities, if they existed at all.

However, more and stronger encryption has undoubtedly become increasingly available. Digital devices, including smartphones, now overwhelmingly either come with hard drive encryption on by default or as an option to be enabled. Popular messaging services, including WhatsApp, iMessage, and Signal, offer end-to-end encryption by default, meaning the provider does not maintain a means to access the content, while other services offer end-to-end as an option.[16] And as the deployment and sophistication of encryption has increased, so, too, have the threats that people face in the digital environment. Massive data breaches are a regular occurrence, reported on the front page of newspapers around the world. Device thefts are also a common problem, with thieves looking either to exploit the data on the device or resell the device itself (or both). Strong encryption is the first, and possibly best, defense against many of these threats and others.

STRATEGY AND METHODOLOGY

Today, there are essentially two sides in the debate on encryption: those who say that it must be possible for government agents to get access to communications when needed (though there are disagreements over what type of "communications" are being sought), and those who insist that such access cannot be provided securely or without high costs to privacy and commerce. In order to facilitate conversation between these two camps, the Crypto Colloquium started with a single assertion: that there are technical means to build systems that ensure the availability of content to government officials within specified contexts.

Participants were asked, regardless of their position, to assume that such a system was mandated by law. Following an initial discussion, participants agreed on six pre-conditions to frame the conversation about the mechanism:

1. the need for officials to act in good faith in invoking it;
2. the requirement for it to be written into law, but that the law would not mandate any specific mechanism;
3. the need to respect current legal standards;

[15] https://www.epic.org/crypto/clipper/.

[16] This does not represent an endorsement of any of these services nor a guarantee of their security.

4. clearly defined rules for minimization and handling of data;
5. that it would be limited to encryption on devices; and
6. the implementation of the mechanism would be tied to the cellular network.

Participants disagreed about whether the mechanism under discussion would require a company to perform a function or turn over data, with no resolution to the question and the remaining conversation covering both options.

To help ground the discussion, the participants decided to limit the conversation to encryption on devices, not messaging applications or other systems that enable transfer of communications data — e.g., they agreed to discuss the issues surrounding encryption for smartphones like the iPhone, but not chat services like WhatsApp. U.S. government agencies have identified the inability to access information on encrypted mobile phones as one of the biggest current challenges to criminal investigations. Last summer, participants in a workshop hosted by the National Academy of Sciences (NAS) began a review of potential access mechanisms law enforcement could use for this purpose. Enabling participants to confront a specific challenge identified by law enforcement, and to build off the work done by NAS, allowed for narrowing the scope of the issues at stake, facilitating the catalog and clarification of the potential benefits and risks.

With these circumstances in mind, the conversation then focused on three issues: what impact would the mechanism have on law and policy? On security? On the economy? Participants were asked in separate sessions on these three questions to engage with one another, and with the topic, to produce a thoughtful analysis.

In order to facilitate openness, the conversation was held under Chatham House rules. That means that quotes by participants will not be included here without the speaker's permission and no attribution will be made to a specific participant.

Lessons Learned

The bulk of the Crypto Colloquium was devoted to discussing the legal, security, and economic consequences of a mandate to ensure government access to content information on devices. While these conversations overlapped in several, meaningful ways, they each produced important observations that the participants largely agreed upon, although not necessarily unanimously. Below we provide a summary of those lessons learned, as well as some more general "unanswered questions" that participants identified as needing more research and analysis.

LAW AND POLICY

Current U.S. legal standards and practices may not be adequate

Participants broadly agreed that, if an exceptional access regime were mandated, it should require at least a probable cause warrant to invoke the use of the mechanism. They did not agree on whether the warrant standard alone was strong enough. One participant recommended inclusion of all or some of the U.S. statutory requirements for wiretaps,[17] which supplement the probable cause standard. Several participants agreed that authorities should not be able to invoke such a mechanism remotely (analogized to government hacking).

Also discussed was which entities would be able to invoke exceptional access, and participants debated the degree to which giving state or local law enforcement the authority to use a mechanism without a federal overseer would increase security risks. On the flip side, they also pointed out that an overseer might bottleneck the process, greatly increasing the potential for delay in legal process. Several participants discussed transparency and nondisclosure orders (gag orders) as well as the capacity for companies to challenge any requirement.

Finally, participants raised the question of constitutionality and asked whether any potential regime could survive review in light of the impact it would have, *inter alia*, on the First, Fourth, and Fifth Amendments. Several participants raised further questions about adherence to the particularity requirement for searches in the Constitution and at least one endorsed the need to forgo any reliance on the "plain view" doctrine to extend the outer limits of a search warrant. This concept is related to that of "proportionality" in human rights law. As one participant explained, precedent from the European Court of Human Rights on the requirement for proportionality may render any mandate that companies build in mechanisms that impact every user in contravention of international law.

The U.S. position on encryption will influence other governments

Participants broadly pointed out that any action, or inaction, will likely influence steps taken by other governments. For example, one participant observed that the United Kingdom, among other nations, is positioning itself as the leader on encryption policy and, with the passage of the Investigatory Powers Act, is currently implementing authorities that could force companies to undermine encryption. A participant pointed out that officials in both

[17] 18 U.S.C. § 2511, available at https://www.law.cornell.edu/uscode/text/18/2511.

China and Brazil are, either purposefully or not, using factually inaccurate information about U.S. law to justify their own laws and policies. Participants also made clear that regimes in these other countries would not be able to rely on protections in U.S. law or the Constitution. China was identified as a big problem actor.

One argument presented in favor of a U.S. regime was that it could set the international standard that others would then rise to meet, but a participant pointed out that nothing would stop officials in other countries from passing separate mandates, and that this may put companies in a position of having to create several different products to comply with conflicting requirements. Given the existence of other regimes, a third participant indicated that any U.S. regime should not be seen as an overall worsening of the ecosystem.

Relatedly, other participants discussed how other governments are reacting by taking strong positions in support of encryption. Here, one explained, a U.S. regime could be brought for review in the European courts, raising unique legal questions.

Exceptional access regimes will be replicated

In discussions about the impact of U.S. conversations internationally, participants generally agreed that any U.S. system would likely be replicated by others. One specific solution discussed was an access mechanism in each phone that qualifying government regimes could invoke using geographicallytargeted technology. One participant described this colloquially as "Stargate encryption," or, conceptually, one door with one thousand locks. Another participant said that such a system would add "significant complexity," in turn increasing vulnerability. However, as one participant explained, while there may be technical ways to limit access to a single phone, there is no way to legally prevent any government, including repressive regimes, from exploiting that access. Further, as another participant explained, in other contexts the U.S. cannot decide which governments to partner with, so it's not clear the government would be able to do so here. Another countered that it would be better to replicate a U.S. system than a bad system designed somewhere else, although several participants also pointed out that scaling any system internationally would introduce additional security risks.

One participant proposed dealing with replication across countries by adding an artificially significant cost, which would act as a barrier to some governments, limiting the number of times the mechanism would be invoked. Another wondered whether new limitations could be built into the Electronic Communications Privacy Act, while conceding that this would create choice of law problems and would likely be rejected outright by the international community.

International obligations will require that mechanisms can be disabled

For a variety of reasons, many participants coalesced around the conclusion that any exceptional access mechanism installed in hardware would have to have a feature that allowed it to be disabled when a device crossed borders. The cellular network was discussed as a means to enable and disable the mechanism. One participant grounded the necessity for such a capability in the need to establish user trust and address security issues; another explained that if the mechanism were turned on in certain jurisdictions, conflicting legal obligations would create problems.

This created hard questions for some, including whether high-value targets would be able to take advantage of the capacity to disable the mechanism, finding ways to turn it off and avoid its being used against them. Other questions included whether mechanisms would be keyed to location or citizenship, whether and how government could mandate mechanisms for foreign-bought hardware, and how to measure the implementation costs at scale.

Exceptional access mechanisms may be only a short-term and / or partial solution

Several participants raised questions about the trends in technology as well as the reach of any regime. This led to agreement that no single solution would solve all problems, or even any specific part of the problem for any period of time. Based on this conversation, several participants agreed that any legislative solution must come with a sunset. Several participants discussed, but did not reach consensus on, whether a mechanism should target less sophisticated criminals, or if it should be designed to reach the more experienced as well, and how necessary or effective it would be in either case. One participant questioned whether some companies would eventually take steps voluntarily to ensure that they build systems in a way to provide for access, in response to regulatory threats, and to preserve the avenue of self-regulation.

SECURITY

Tools will always be developed and used outside of any regime

Nearly all participants agreed that any plausible regime would leave loopholes that would allow people to avoid the exceptional access mechanism. Several participants gave examples of these loopholes and how they could be exploited. For example, a mechanism tied to the phone network could be avoided by keeping a phone on airplane mode and only connecting over wifi. One participant pointed to the prevalent use of Virtual Private Networks (VPNs) in China to bypass the content and access restrictions as evidence that such avoidance would likely be the outcome.

There is a gap between what is technologically possible and politically feasible

Participants generally disagreed over whether any mandate written into law would have to be broad or targeted. One participant indicated that the former would be unreasonably expensive and the latter too easy to work around. However, participants were able to agree that any legislative text would be highly controversial and not likely to get the support it would need to pass.

Implementation could mean discontinuation of tools and technologies in use

Several participants provided details about security tools currently built into popular products and services, as well as developments that are expected in the coming months, all of which would have to be significantly altered or discontinued under an exceptional access regime.

This would mean that both the investment that these companies made in these tools as well as the security benefits that users currently enjoy — which many participants recognized as significant — would be lost. It would also require that these companies invest in research and development for means and methods to replace these tools that would comply with the regime, and in the case of some hardware providers, it could also require investment in retrofitting devices that are already on the market.

Any regime will bear high costs in terms of coordination and resources

Without reaching total agreement on the extent or nature of those costs, participants agreed that an exceptional access regime would impose significant costs on both the government and private sectors. One participant explained that a system that was based on the cellular network would — or at least should — require research and investment in patching any known vulnerabilities in that system, including those associated with Signaling System No. 7 ("SS7").[18] Others discussed the cost of buying new equipment, the security impact of companies investing less in tools outside the regime, and the outlay of time and resources to review applications that users might be able to use on a device to undermine the mechanism. Participants pointed out that these costs would likely prohibit potential competitors from entering the market.

The costs associated with losing consumer trust was a major topic of conversation. A participant discussed the "statistical certainty" of security flaws due to bad implementation of a mechanism, at least in cheaper phones, although some disagreed. The cost incurred by long-term economic stunting of the market due not only to domestic but also international loss of user trust was raised by another participant.

In terms of mitigating some of these costs, some discussed whether it would be possible to do so within the regime, though solutions were not proffered.

Security of a mechanism will vary depending on frequency of use

While little detail was discussed, most participants agreed that there would be a relationship between the general security of a mechanism and the details of how it could be invoked. For example, a mechanism that would be used frequently or one that could be used by more people would have a higher risk of being exploited. One reason that participants discussed was the additional complexity of a mechanism used more frequently, with a participant explaining that complexity is inapposite to security. One participant responded by saying it is necessary to consider the scale of the problem and the burden it would create to have only a small number of individuals with authority over the mechanism.

[18] https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls.

Mechanisms will disproportionately impact poor and marginalized communities

One participant, with agreement from several others, described how any exceptional access regime would represent a civil rights issue, with disproportionate impact on low income and marginalized populations. Specifically, the participant explained that even if sophisticated device manufacturers can make the mechanism secure, those who operate on the lower-end would not be able to do so, with the potential of a misstep being particularly great in the implementation phase. Another participant flagged that this issue would also impact activists and poor populations in other countries.

ECONOMICS

Methods to empower users may provide the same function as an access regime

Several participants highlighted ways government agencies and officials could invest in systems and resources not facially related to encryption that would provide better tools to empower users and, as a secondary effect, also offer another channel to pursue information in official investigations and inquiries. One option discussed was putting more focus on post mortem estate planning for devices and accounts holding digital information; another was the continued use of biometric schemes to unlock devices. A participant noted that consumer preferences and the market are already designing and creating tools, like cloud storage and escrowed passwords, that were not designed with the intention but have the effect of opening paths for government agents to gain access to content.

Companies subject to regimes will be at an economic disadvantage

A large majority of participants agreed that a system where only certain companies are required to build in access mechanisms — as any system must be, practically — will economically disadvantage those companies. Costs discussed included the general financial costs of research and development, and new hardware, particularly at scale; the cost in loss of trust and, by extension, customers, particularly in the international market; and the cost in terms of regulatory compliance with laws in other legal regimes. Several participants agreed that for smaller companies, these costs may be prohibitive.

One participant raised the question of government compensation for some of these costs, although another countered that, in general, compensation is limited to assistance and not funding to build the capability. A participant also brought up the trickle-down impact of exceptional access regimes, namely that they would impact users' trust not only of the service or device in question, but also anything that relies on the device. For example, digital wallets rely heavily on the security of the device and any mandate for the device would impact its security. Finally, in contrast, one participant questioned whether an exceptional access regime could be designed in a way to incentivize the provision of increased security for users.

Users will still be able to work outside exceptional access regimes

The corollary of having companies that are not subject to an exceptional access regime is that users will have options available outside of that regime. Specifically highlighted by many participants is the ever-expanding market of secure app-based or "open source" tools, particularly those that are community led and developed. Others mentioned manufacturers outside the United States as well as the "black market" as sources for users looking for either more secure or more private tools. One participant flagged that cultural issues may, in some cases, provide the basis for choosing or developing other tools or technologies or, in more extreme cases, for walking away from the market entirely.

Technology-specific mechanisms will require frequent updates

Participants reached broad consensus that any access regime that dictated any specific technology would be, in the words of one participant, "a disaster."

Perception of a regime could influence other companies and governments

Regardless of the implementation, many participants said that how a regime is perceived externally could have wide-ranging influences. One participant supported this conclusion by pointing to the reactions following the Snowden revelations in 2013. One possibility discussed was that companies might relocate offices or factories to countries without a legal requirement for access in order to regain consumer trust and avoid the appearance of complicity with a "U.S. intelligence operation." In response, someone noted that the capacity to disable the mechanism might counter some of this negative perception. In contrast, several participants said that government responses could lead to the pursuit and implementation of more and different access mechanisms, many of which would likely further undermine rights and security, and greatly exacerbate problems created by the existence of any single regime.

UNANSWERED QUESTIONS

What is the preferred reach or effectiveness of an exceptional access regime?

Early on in the discussion, participants highlighted the lack of public information about what specific goals government agents are seeking to achieve through an exceptional access regime. For example, one participant asked whether it was better "to hit a 60% solution and not a 90%?" Another explained that it is hard to "proffer any solution without a set problem," and a third noted, in agreement, that many people have already participated substantially in conversations on this topic and observed that government officials should now take steps to explain what their proposed solution is, rather than asking others to "build impossible things." To counter this narrative, one participant explained that the right conversation hasn't

happened in the right environment to determine "policy boundaries in which a technical solution would operate."

Participants asked specifically about the degree of sophistication that should be necessary to bypass an access mechanism and pointed out that advances in technology would likely make it so less and less skill would be required. A participant asked whether this was simply a question of defaults or if government officials were looking for a regime that would need to go beyond that.

How do government agencies face encryption both as a barrier or asset?

Participants spent a significant portion of time exploring what information government agents can already access under most circumstances even when a device is encrypted, simply by using several separate warrants. Participants heatedly debated the scope of information that is available, when content is stored with other companies (like application providers), there are cloud backups, and metadata for analysis. They were unable to reach any conclusion on what pieces of information might be missing. Several participants, however, were adamant that these alternate routes do not provide what is necessary, and at least one participant flagged that the other routes are overly time-consuming. And, as one participant explained, regardless of the present situation, several application developers are moving toward adopting data minimization as a policy. This means that companies are starting to retain less data. Another participant posited that there are likely more services coming that law enforcement and intelligence agencies must grapple with.

Expanding the conversation, other participants said that there is not enough information publicly available regarding the rate or frequency of cases in which encountering encryption has impeded an investigation. Participants called attention specifically to the misleading nature of the data and statistics that are currently available, which do not specify when encrypted data was both necessary and not otherwise available and do not include cases where agents did not pursue authority to search a device because they already knew that encryption would prevent access.

Generally, participants conceded that this type of data may be largely subjective. One participant discussed using a "failure to convict" accounting, but many thought there was space for further discussion. However, ultimately, several participants emphasized that getting this data is important for establishing the scale of the issues, as well as to identify priorities for any ongoing discussions.

What are the actual costs of exceptional access to personal and digital security?

Several participants who discussed the lack of information available from government agencies also flagged, on the flip side, the need for more information to quantify the impact of encryption in minimizing the harm from data breaches and in supporting information security more generally. One participant flagged 2013 research on the number of stolen phones that resulted in identity theft, while another saw opportunities in looking at the adoption of security tools and assessing their impact.

Where and how does liability get assigned in an exceptional access regime?

Many participants raised the open-ended question of liability. Some questioned whether it would ultimately fall on the individual, while others thought it would fall on the provider, and at least one participant thought government agencies should be held accountable for any breaches. A participant discussed the problem of incentives when a one party bears the costs while a different party gets the benefits, and specifically asked that a system not seek to absolve liability for entities that make mistakes. Some participants discussed concepts of partial or joint liability and of insurance models that could cover this space. Ultimately, participants generally believed that the party that bears the responsibility for creating and maintaining the system would likely incur significant legal, financial, and security duties, the extent to which should be answered by law.

Conclusion

The fruitfulness of the day's conversation demonstrated that making specific assumptions and setting a common fact pattern was useful to promote consensus from across stakeholder groups as well as to identify where more discussion could be helpful. Substantively, a prevailing theme from the day was that any solution, were a solution developed, that was designed to meet the current stated needs of U.S. government agencies, even in the narrowly constrained fact pattern discussed, would likely be effective for only a minimal time, would be substantially costly, and might harm security in general. These are significant hurdles that cannot be casually dismissed, but should instead be confronted honestly by anyone pressuring companies to implement bypass mechanisms. While further research is certainly required to provide concrete data points, the bulk of the discussion argues against any movement to implement an exceptional access regime.

NEXT STEPS

While the United States could, in many ways, be described as "ground zero" for the debate on encryption, it is not the only place where the discussion is currently playing out. Countries around the world, from Australia, to India, to Brazil, to the United Kingdom, are now debating whether they can or should compel companies to take action to ensure access. The coordinators of this report will seek to share the lessons learned here with leaders in law and policy in these other countries, as well as with people in inter-governmental bodies, like the "Five Eyes" intelligence partnership and the Organization for Economic Cooperation and Development (OECD).

MORE INFORMATION

For more information on anything in this report, you can contact the event organizers: **Amie Stepanovich** (amie at accessnow dot org), **Nathan White** (nathan at accessnow dot org), or **Camille Fischer** (camille.fisch@gmail.com).

Crypto Colloquium: Lessons Learned on Encryption in the United States

January 2018

accessnow