WINTER 2022 / ISSUE NO.20

$ 15.00 | € 10.00 | 1500 RSD

HORIZONS

ISSN 2406-0402

JOURNAL OF INTERNATIONAL RELATIONS AND SUSTAINABLE DEVELOPMENT

A CYBER ODYSSEY

QUANTUM OF HOPE

cirsd.org

The Conflict over Cryptography

Battling over Differing Versions of Security

Susan Landau

REVOLUTIONS are messy things, and the Digital Revolution is no exception. It has created new opportunities and new risks, new centers of power, and, in a truly revolutionary style, serious new threats that allow attackers from half a world away to threaten—and sometimes cause—serious damage without physically crossing a border. It has also allowed new types of crime to flourish.

Some regimes—including Russia, China, and Iran—that seek information security as well as cybersecurity are building their own internets in order to limit access to the rest of the world and restrict the ability of information to transit borders. Other nations, supporting the free flow of information, want cybersecurity—in contradistinction to what is called information security. They are struggling to prevent cyber exploits (theft of data), cybercrime, and cyberattacks from within and outside their borders. Here is where the conflict about cryptography arises.

Cryptography secures communications and protects data at rest—but that very same technology can also complicate, and even prevent, criminal investigations. It can hide the tracks of spies. For years the battle over the public's use of strong encryption technology has been described as a battle over privacy versus security. But that description misses how our society has changed and how reliance on ubiquitous, easy-to-use cryptographic systems—iMessage, Signal, automatic secure locking of smartphones, and so on—are necessary not just for individual privacy but to provide security. Widespread use of cryptography enhances national security, public safety,

Susan Landau *is Bridge Professor of Cyber Security and Policy, The Fletcher School and School of Engineering, Tufts University. She was previously a senior staff privacy analyst at Google and held the post of Distinguished Engineer at Sun Microsystems.*

Photo: Photo Stock

security from hostile foreign actors—and, yes, privacy. The cryptography debate is really a debate about security versus security. And that makes it very complicated.

Battles over the public use of strong encryption systems started in the 1970s, when public-key cryptography first made its appearance. A cryptosystem has two parts: the algorithm, or method of encryption, and the key that is used with it. Here we can give the well-known Caesar shift system as an example. In this system, each letter is shifted—an "a" in the unencrypted version becomes a "D," a "b" becomes an "E," etc.—where "shifting" would be considered the algorithm, while "3" would be considered the key, since each letter is shifted three letters. A more interesting encryption system is a substitution cipher, in which the letters are randomly mixed: an "a" might become a "T," a "b" an "F," and so on. In this case, the algorithm is the substitution, and the key is the table that reveals that an "a" becomes a "T."

Since the late 1800s, the basic tenet of cryptography has been that the encryption algorithm should be public—many eyes viewing it can help ensure that the method is actually secure—but that the

encryption keys should be kept private to the people who are actually communicating. That made the issue of "key exchange" complicated because security dictates that keys should be frequently changed. Otherwise, it becomes easier for an adversary to discern patterns and thus decrypt captured messages.

Bedevilments and Battles

Key exchanges bedeviled cryptographers. It is one thing when two people can agree on an algorithm and exchange keys in person before they need to communicate confidentially, but quite another if they run out of keys. This happened to the USSR during the Second World War, when it could not supply its embassies with fresh cryptographic keys. Its diplomatic representations reused keys, which allowed the National Security Agency (NSA) to later decrypt communications they had collected from encrypted Soviet transmissions sent during the war.

With the arrival of the internet, it was not just diplomats and spies that needed secret key exchanges—everyone did.

With the arrival of the internet, it was not just diplomats and spies that needed secret key exchanges—everyone did. For example, when you choose to buy something from a website, you need to protect the credit-card number you submit. But how do you do that if it's the first time you have ever been to that website? Public-key cryptography, which is based on problems that are fast to compute but much slower to reverse, provides the mathematical magic enabling secure key exchange. When Stanford and MIT computer scientists developed the idea in the mid 1970s, the national-security community pushed back; they had been the ones doing cryptographic research, not university professors or industry researchers, and they expected to continue to own it.

Thus began many decades of battles over the public's use of strong cryptography—cryptography hard to undo except by trying all possible keys (a so-called "brute force" attack). The NSA first tried to prevent publication of research in cryptography, then it sought to control government development of cryptographic standards, and finally in the 1990s, it used export controls to slow the deployment of cryptographic systems. Such control also slowed the use of strong cryptographic systems within the United States, a result that had strong FBI support. Because the European Union had similar export controls, it was difficult for the public to obtain communication or computer systems with strong cryptographic capabilities.

Then, in the late 1990s, the situation changed. American industry had been pressing the U.S. Congress to lift the imposed controls. Meanwhile, the NSA was discovering that it was not just technologically-sophisticated countries that were deploying strong cryptography; many less technically sophisticated states were as well. The NSA needed to move to other methods, namely Computer Network Exploitation (CNE), to gain access to other nations' information. Basically, the NSA made a deal with Congress: it would not oppose a change in the regulations that would allow American companies to export systems with strong cryptography so long as the systems were not custom-made or sold to governments or telecommunications providers. In exchange, the NSA would receive government support to increase its CNE capabilities (the NSA's success in the latter is clear from the Edward Snowden disclosures). The EU, informed of the intended U.S. policy change, similarly loosened its export control requirements on cryptographic equipment, slightly prior to the U.S. modification. The FBI was not happy about this change, fearing that its ability to wiretap would quickly disappear. That did not occur, at least not immediately. In fact, at that time mobile phone providers did not even encrypt the radio transmissions between a mobile phone and cell tower.

With the change in cryptography controls, many computer scientists expected an avalanche of tools enabling end-to-end encrypted (E2EE) communications.

With the change in cryptography controls, many computer scientists expected an avalanche of tools enabling end-to-end encrypted (E2EE) communications (encrypted from the user to the receiver, thus preventing an interceptor from reading the message). Developed in the 1990s, PGP encryption could do so, but its architecture and interface presented barriers for the technology to become widely used by consumers. Instead, the first mass use of encryption turned out to be in securing phones.

Mobile Phones Lead the Way

Apple launched the iPhone—both a phone and a computer—in 2006. The phone became popular quickly, especially after Facebook became available to the public in 2007. The phone also caught on quickly with thieves, who found the small, expensive device easy to steal and resell. Apple countered by developing a feature called Find My iPhone, which caused theft rates to drop (Android's equivalent, developed later, is Find My Device). But in the late 2000s, criminals had a new wrinkle: stealing data off lost and stolen devices, then using the information for identity theft. Securing the data on the phone became quite important.

Currently, out of the five U.S. companies that hold a dominant role in the Internet economy—Facebook, Amazon, Apple, Microsoft, and Google—Apple stands out because it is a hardware company. While Apple produces great software, the company's profits come from selling hardware: iPhones, iPads, iMacs, and the like. This implies that Apple looks at customers differently than Microsoft, which focuses on selling software, as well as Facebook, Amazon, and Google, which focus on selling whatever their advertising networks convince the consumer to buy.

Apple sought to move into the corporate marketplace, and that meant emphasizing security; the company wanted its devices to be fully private, which is also a form of security.

To a company that focused on selling hardware, such tracking of users was not particularly useful. Indeed, it was actually counterproductive. Apple sought to move into the corporate marketplace, and that meant emphasizing security. Corporate security included wiping data if phones were lost or stolen. Apple's vision went further; the company wanted its devices to be fully private, with only the user able to access information on them. Such privacy is also a form of security.

In 2008, Apple began working towards a system in which only the legitimate user could open the phone and access its data. This solution would prevent criminals from pulling personal and business data from lost or stolen phones. With the 2014 release of iOS 8, one would need the user's PIN to unlock around 90 to 95 percent of the phone's data (Apple could, of course, access data that the user stored in the iCloud). With the 2015 release of iOS 9, Apple made it much harder for anyone but the user to access data on the phone; the company designed the phone to erase its data after ten incorrect tries of the user PIN.

Though these protections increased security—and thus prevented certain types of crimes—they did not please law enforcement. FBI Director James Comey began giving speeches objecting strongly to Apple's security enhancement.

The conflict between Apple and the FBI over secure phones came to a head in 2016. Two terrorists had attacked a San Bernardino Health Department holiday party; the terrorists themselves were killed in a police shootout a few hours later. The terrorists had destroyed their personal phones and computers but left behind a locked work iPhone secured through the iOS protections. Law enforcement wanted the device opened.

The FBI argued the phone might contain critical data about the dead terrorist's contacts and sought Apple's help to counter the security protections built into the operating system in order to access this information. Apple replied that it was not under a legal obligation to do such extensive rewriting of its system and that, furthermore, there was a serious risk that developing such software would create undue security risks for all its phones. When the company refused to comply, the government took Apple to court. The case was mooted after an FBI consultant found a way around Apple's protections and unlocked the device.

The real issue was law enforcement seeking so-called "exceptional access"—access for law enforcement under court order—to secured mobile phones.

The FBI found no evidence on the phone, but that was not the real point of the battle. The real issue was law enforcement seeking so-called "exceptional access"—access for law enforcement under court order—to secured mobile phones. Ever since the change in export control laws, the FBI had been seeking ways to limit the domestic use of encryption. Arguing that law enforcement was "going dark" due to encryption preventing eavesdropping on wiretapped communications, the FBI sought relief through legislation or the courts. Now the FBI added the category of secured phones to the issue. Law enforcement outside the U.S. echoed the FBI's complaint. Some—but not all—national-security agencies added their voices to this as well.

There were also some striking opponents to the FBI's push for exceptional access. This included Former NSA Director Mike McConnell, former Secretary of the Department of Homeland Security Michael Chertoff, and former Deputy Secretary of Defense William Lynn III, who wrote in a *Washington Post* oped that "we believe the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server, and enterprise level without building in means for government monitoring." Another former NSA Director, Michael Hayden, told an interviewer that "we are probably better served by not punching any holes into a strong encryption system—even well-guarded ones." This viewpoint was echoed outside the United States, as well. Robert Hannigan, former director of the UK's Government Communication Headquarters said at a meeting at MIT: "I am not in favor of banning encryption. Nor am I my asking for mandatory 'back doors.'"

From Escrow to Exceptional Access

The fight over access to end-to-end encryption emerged in the 1990s. In 1993, the U.S. government proposed "Clipper," a system for encrypting digitized voice communications where the encryption keys would be split and stored with agencies of the U.S. federal government. This proposal garnered

support neither from foreign nations nor from American industry or private citizens.

Many objected to the fact that storing encryption keys with U.S. government agencies eliminated communications privacy despite the legal protections that the government pledged to include in the system. Others raised security objections. End-to-end encryption systems are designed to prevent intrusion, while the proposed escrow system would be at risk of compromise by those running the system. A more serious concern was that concentrating encryption keys in storage systems provides a rich target for attackers. Finally, escrow systems destroy "forward secrecy," in which keys are used for a single communication, then destroyed at the end of the communication. Such systems increase security while lowering costs, since the keys are needed only during the communication and are not stored afterwards. If communications are protected using forward secrecy, an attacker who gains access to keys will be able to decrypt data from that time until the breach is discovered and patched. The attacker would not be able to decrypt any previous communications because those keys were destroyed after use. Escrowing keys changes that calculus, increasing risk.

Widespread use of cryptography enhances national security, public safety, security from hostile foreign actors—and, yes, privacy. The cryptography debate is really a debate about security versus security. And that makes it very complicated.

The Clipper system did not catch on, and the U.S. government abandoned the idea in the late 1990s, shortly before the change in export controls. However, the FBI and U.S. law enforcement did not give up on the idea of accessing encrypted communications. They began to push for something called exceptional access instead.

Unlike escrowed encryption, exceptional access is not a specified technology. Instead, it is the belief that encryption systems could be designed to be secure yet enable legally authorized surveillance. Such an expectation flies in the face of what computer security experts have learned in over 50 years of designing secure systems.

The biggest problem stems from the complexity that an exceptional access system introduces. Such systems would be far more complex than the E2EE systems in use today and—as engineers know—this increases the risk of vulnerabilities. Furthermore, there is the issue of jurisdiction. In the case of the Clipper system, the issue presented itself as the proposal's inability to handle differing rules for differing jurisdictions. Which laws and whose access would apply in a trans-border phone call, for example?

Implementing exceptional access for a mobile phone bought in one country, used in a second to make a call to a third, is enormously complicated. Would there be a single regulatory environment? Would there be multiple ones? Such questions would need to be answered before an exceptional access system could possibly be implemented.

The NSA spying revelations created a breach between the U.S. technology companies and the government that lasted several years.

In addition to those problems with exceptional access systems, there were also other issues. Requiring exceptional access would mean eliminating forward secrecy, which immediately decreases security. Exceptional access would also put an end to "authenticated encryption," a technology that securely combines authentication (ensuring that the message has not been tampered with during transit) and confidentiality (ensuring the privacy of the communication). In the 1990s the two functions were done separately; combining them helped eliminate errors that caused vulnerabilities. But exceptional access would necessarily separate the two functionalities.

Snowden and Spyware

The 2013 Snowden disclosures, with their revelations of the vast collection and capabilities of the NSA, silenced U.S. law enforcement for several years. The issue was not in responding to court orders for customer content; the companies had done so, of course. Snowden revealed that U.S. technology companies had been targets of bulk collection, with the NSA siphoning data "wholesale" from tech company overseas data centers. Google, Yahoo, and Microsoft doubled down on securing their intra-company communications, and the public too began to think more about securing their own. The NSA spying revelations created a breach between the U.S. technology companies and the government that lasted several years.

In 2015 the Obama administration considered the law-enforcement arguments—and opted not to propose legislation on encryption. The rationale behind the decision included benefits to civil liberties and human rights, a potentially positive effect on U.S. economic competitiveness, and increased security through broader use of encryption, even while acknowledging that such broader use could potentially impede law enforcement efforts. One sentence in a draft options paper for the U.S. National Security Council paper was particularly striking,

"[B]ecause any new access to encrypted data increases risk, eschewing mandated technical changes ensures the greatest technical security." In other words, American national security interests are best protected through the broader use of encryption throughout the infrastructure—and that is best done through encouraging industry's implementation of strong cryptosystems. The message between the lines was that the U.S. national security and law-enforcement interests had diverged on encryption. To be fair, part of the reason for this divergence was national security's greater ability to work around encryption, a skill that law enforcement largely lacked.

It was not altogether surprising that despite the protections built by Apple, an FBI consultant was able to unlock the device of the San Bernardino terrorist.

Other nations did not see the situation the same way. The UK government has continued to press for access to both content and devices. Australia passed a controversial telecommunications law that appears to include the government's ability to require companies to build capabilities to get around encryption—"appears" since that aspect of the law had not been contested in court at the time of this writing. Some nations, such as Russia and China, strongly restrict the use of encryption technologies. Most democratic nations do not, although discussions about doing so occur in the European Union as well as in the UK and other nations.

Returning to the issue of locked phones, it was not altogether surprising that despite the protections built by Apple, an FBI consultant was able to unlock the device of the San Bernardino terrorist. Cellebrite, an Israeli company that had started its business providing phone-to-phone data transfer, begun offering smartphone forensic tools in 2007. Police departments and governments were among its customers. In 2018, *Forbes* reported on Grayshift, a company focused on hacking iPhones whose customers included the FBI. Use of vulnerabilities to break into digital devices was not a new direction for law enforcement; the FBI had used court orders to conduct such searches since the early 2000s.

Other organizations were also successfully hacking into iPhones and Androids. The Israeli company NSO Group developed a sophisticated spyware called Pegasus that is installed through vulnerable apps or spear-phishing and, more recently, through a missed call on WhatsApp. The company claims it sells only to governments for legitimate investigations, but for over a decade NSO software has been used to target human rights activists, journalists, and political opponents of regimes (as well as their family members and friends).

In short, despite all the protections that Apple and Google had built for the phones, smartphones remained less than fully secure, especially against a determined and skilled attacker. At the same time, even when locked, the phones remained a particularly rich source of information for investigators. Users carry their mobile phones everywhere, which means that the cell tower records have approximate information of where users have been. Such proximity and location information has proved invaluable to investigators, helping them, for example, to determine the identities of a group of bank robbers simply by matching records of cell numbers with the location and time of multiple robberies.

APPS AND INFORMATION

Mobile applications also provide a lot of information. GPS tracking from map applications contains far more precise location information than cell tower sites provide. Other apps might provide other evidence. In one case, a phone showed that a suspect was using the flashlight app for an hour during the time he was believed to be burying a body in the woods. That, along with other evidence found on the same phone, provided definitive proof for his conviction.

Yet sometimes the very abundance of information that smartphones provide can thwart investigations. Smartphones store data that used to be found in other places. The scrap of paper that might have been found in a suspect's pocket listing Joe and his number is now gone, having been replaced by Joe's name and number on the smartphone's contact list—along with all the suspect's other contacts. If the user has backed up his contact list in the cloud, perhaps so he can access it on other devices, law enforcement is in luck, since the data can be collected from the cloud provider under proper legal authorization. Otherwise, information that in the past could have been so easily grabbed from the suspect's pocket may now be quite difficult for law enforcement to access, given the security protections of most recent smartphones.

This type of blockage stood in contrast to law enforcement's experience in the 2000s and early 2010s, a time when phone security protections ranged from minimal to non-existent, and police often examined phones upon arrest. Changes that occurred—increasing security and, at least in some jurisdictions, imposing requirements for a warrant prior to searching phones—created obstructions to conducting legal searches. Police were frustrated. In the U.S, FBI Director Comey's requests that Apple enable access to the phones did not get traction. Forcing Apple to open the phone of the San Bernardino terrorist would have changed the situation.

When that did not happen, the battle over encryption went briefly on hold—but it was not over. The late 2010s saw

numerous changes that brought new pressures to the issue.

WhatsApp introduced end-to-end encryption to its suite of communication applications in 2016; by that time, WhatsApp served as a platform for over 100 million voice calls daily. That transformed seamless end-to-end encryption from a niche product to a tool for the masses. The FBI continued to battle the public's use of encryption. The FBI as well as European legislators raised a new concern—child sexual abuse material (CSAM)—which has been spreading online at a rapidly increasing rate. The material was stored on cloud providers, with users sharing location information through encrypted communication apps, including WhatsApp.

During this period, cyberattacks became more dangerous. The U.S. and Israeli attack on the centrifuges of Iran's Natanz facility in the late 2000s was the first destructive attack on physical infrastructure, but it was soon followed by others, including Iran's attack on Saudi Aramco that erased the disks of three-quarters of the company's PCs. Russian cyberattacks against Ukraine were different in scale, but also showed a willingness and a capability to cause serious physical destruction and damage. Meanwhile, the incidence of ransomware exploded, often targeting critical infrastructure. While cryptography was not the only technology necessary to protect against such attacks, it was an essential piece of security solutions. Consequently, at least in the United States, which continued to be one of several nations most under attack—Ukraine was another—there was little appetite by the national security community for encryption restrictions.

During this period, cyberattacks became more dangerous. Meanwhile, the incidence of ransomware exploded, often targeting critical infrastructure. While cryptography was not the only technology necessary to protect against such attacks, it was an essential piece of security solutions.

The Carnegie Committee on Encryption

In 2018-2019, under the auspices of the Carnegie Endowment for International Peace, a group of senior former U.S. government officials worked with members of industry, civil-liberties organizations, and academia to break the impasse on encryption policy. Many of the members of the committee have assumed to senior positions within the Biden administration, including positions with direct concerns about encryption. I also note that I served on this committee.

The report of the Committee, entitled "Moving the Encryption Conversation Forward," was published in 2019 and it started by abandoning two strawmen: *one*, that society should not try for approaches enabling access to encrypted information, and *two*, that law enforcement will be unable to protect public safety unless it can access all encrypted data.

Today, encryption means many things. To make progress, those of us serving on the Committee proposed splitting the encryption problem into component parts—an approach that makes sense since encrypted communications and encrypted data are fundamentally different technical problems (access to one would not imply access to the other).

We focused on data secured on mobile phones since this issue is of greatest concern to U.S. law enforcement. Another argument for doing so is that currently no approach to encrypted communications fully satisfies cybersecurity, public safety, national security, competitiveness, privacy, and civil and human rights needs while also providing law enforcement access.

We started with principles that technical solutions for law-enforcement access must follow, noting that while we were focused on access to data on secured mobile phones, these principles also apply to other aspects of the debate (e.g., communications):

- *Law Enforcement Utility*: The proposal can meaningfully and predictably address a legitimate and demonstrated law enforcement problem.
- *Equity*: The proposal offers meaningful safeguards to ensure that it will not exacerbate existing disparities in law enforcement, including on the basis of race, ethnicity, class, religion, or gender.
- *Specificity*: The capability to access a given phone is only useful for accessing that phone (for example, there is no master secret key to use) and that there is no practical way to repurpose the capability for mass surveillance, even if some aspects of it are compromised.
- *Focus*: The capability is designed in a way that it does not appreciably decrease cybersecurity for the public at large, only for users subject to legitimate law enforcement access.
- *Authorization*: The use of this capability on a phone is only made available subject to duly authorized legal processes (for example, obtaining a warrant).
- *Limitation*: The legal standards that law enforcement must satisfy to obtain authorization to use this capability appropriately limit its scope, for example, with respect to the severity of the crime and the particularity of the search.
- *Auditability*: When a phone is accessed, the action is auditable to enable proper oversight, and is eventually

made transparent to the user (even if in a delayed fashion due to the need for law enforcement secrecy).
- *Transparency, Evaluation, and Oversight*: The use of the capability will be documented and publicly reported with sufficient rigor to facilitate accountability through ongoing evaluation and oversight by policymakers and the public.

Client-Side Scanning

These principles turn out to be quite applicable to the newest proposed technical solution to provide access to encrypted communications: client-side scanning (CSS). Such scanning has been discussed in the European Union as a possible solution to the CSAM problem.

In 2018-2019, under the auspices of the Carnegie Endowment for International Peace, a group of senior former U.S. government officials worked with members of industry, civil-liberties organizations, and academia to break the impasse on encryption policy.

Scanning of personal content is not new, but until now it has occurred on the server. As cloud storage became cheaper (indeed, often free), users could send links to where these items are stored in the cloud, instead of sending photos or documents to one another. Many cloud providers scan the content stored in their cloud. One reason for doing so is to prevent their servers from hosting illegal content or content that violates their terms of service (Facebook, for example, prohibits displays of nudity or sexual activity). Another is that they may use the information about user interests for business purposes, e.g., to serve ads.

Now, providers are moving to encrypting cloud content, making such scanning much harder. CSS would circumvent this problem, as well as end-to-end encryption, by scanning content on a user device prior to the data being encrypted or after it is received and decrypted. Currently, client-side scanning is being proposed to search for CSAM. However, the fact is that once a CSS system is installed, repurposing what it is searching for is not technically difficult. That creates a serious risk to users. Proposed CSS systems search for "targeted content" that someone has determined should not be on user devices. It could be CSAM, but it could just as easily be political material. The latter is the danger of CSS: as we know well—what one government may label as terrorist materials; another may see as free speech.

Anti-virus systems show us that client-side scanning is not a new technical innovation. But the proposed versions of CSS are substantively different from anti-virus material in a crucial way. Anti-virus software works to benefit the user, while CSS systems check if the user has content on their device that the government deems illegal—implying they do not work for the user but, rather, that they view the user as an adversary.

CSS systems rely on two types of technology to recognize targeted content on a user device. The first is machine learning, which builds models using massive amounts of data to recognize patterns. Machine learning is used in many applications, including spam filters, speech recognition, and facial recognition. The last reveals one of the problems of machine learning systems, which is a high failure rate on data substantively different from the training data. Facial-recognition systems trained on white and Asian male faces do poorly at recognizing women and Black individuals. The other technology is perceptual hashes, which produce a digital fingerprint of a media document such as a photo. If the photo is changed slightly, e.g., by rotation or cropping, its perceptual hash changes only slightly, thus making recognition possible.

Now, providers are moving to encrypting cloud content, making such scanning much harder. CSS would circumvent this problem, as well as end-to-end encryption, by scanning content on a user device prior to the data being encrypted or after it is received and decrypted.

Proponents of client-side scanning systems argue that the systems protect privacy—only targeted content is subject to legal action—while enabling law enforcement to have a workaround against encryption. But a deeper analysis shows that neither premise is correct. It is beyond the scope of this essay to discuss these technologies in detail, but I will note that both machine learning and perceptual hashes are subject to false-positive and false-negative attacks. The former occurs if an adversary produces an image that appears to match the targeted content but actually differs in substantial ways. The latter occurs if an adversary produces an image that is, in fact, targeted, but has changed the image in some minor, yet critical way that fools the algorithm (either machine learning or the perceptual hash mechanism). False positives mean that a user may appear to be hosting illegal content although he or she is not—and data on his or her devices may be subjected to searches without legal cause. At the same time, sophisticated criminals—and CSAM purveyors appear to be skilled at using modern anti-surveillance technology—will be able to evade the CSS system.

There are even more concerns surrounding CSS systems. To work, they must be installed on *all* devices, not

just those suspected of carrying targeted content. It is relatively easy to reprogram a CSS system from searching for CSAM content to searching for "tank man" photos. In other words, CSS systems can be repurposed from serving as CSAM detectors to serving as bulk surveillance tools. Think back for a moment to the principles from the Carnegie encryption policy study; it is immediately clear the client-side scanning violates several of them, including *utility*, *equity*, *specificity*, *focus*, *authorization*, and *limitation*. Many of the arguments for pursuing CSS is the inability to make targeted content public—but that same argument then presents serious problems to fulling the auditability, transparency, evaluation, and oversight principles. To put it simply, far from protecting it, CSS raises serious risks to privacy—and security.

Proponents of client-side scanning systems argue that the systems protect privacy—only targeted content is subject to legal action—while enabling law enforcement to have a workaround against encryption. But a deeper analysis shows that neither premise is correct.

Strong Encryption

The encryption debate has been ongoing for almost half a century. It started with who "owns" encryption and continued with whether the public should have the ability to keep its communications and data secure, even if that sometimes blocks legally authorized government investigations. The debate became more public and strident over the last decade, in part because the Snowden disclosures revealed far greater collection than had been understood. The wider availability of secured devices and communications, which genuinely makes investigators' jobs more difficult, contributed even more to the heated discussion.

Where do we sit at the beginning of 2022? SARS-CoV-19 turned the world upside down in 2020; one lesson we quickly learned as we transitioned to working from home was the need for widely available, easy-to-use strong encryption in consumer devices. I wrote in 2016 that, "if breakable encryption is the only permitted encryption solution, it will not only be the U.S. government that reads the communications of American companies and others, but also the Chinese, the Russian, the Iranian, the French, and many others. And they will do so with or without court orders." The proliferation of cyber exploits and cyberattacks since then serve only to emphasize the importance of availability and use of strong security through the infrastructure—and that includes strong encryption.