February 10, 2015

The American Civil Liberties Union thanks the Special Rapporteur on the Promotion and Protection of the Right to Freedom of

a. How encryption works.

Modern encryption provides a way to scramble information so that only someone who knows a secret can unscramble it. In its unscrambled form, the data is known as "cleartext," and in its scrambled form, it is known as "ciphertext." The secret that allows the unscrambling is known as a "key." The ciphertext can be stored ("data at rest"), transmitted over a network ("data in transit"), or both.

The main goal of encryption is to hide the cleartext from anyone who does not have the key, including from any adversaries who may have access to the ciphertext.

b. Symmetric and asymmetric encryption.

There are two common forms of encryption relevant here: symmetric encryption and asymmetric encryption.

Symmetric encryption uses the same key to both encrypt and decrypt. It can be used by a single party: for example, to lock their own data in storage so that only they can retrieve it. Or it can be used by multiple parties: if two parties share a key, they can use symmetric encryption to send messages to each other that no one else can access without the key.[1]

In asymmetric encryption, by contrast, the key for encryption is different from the key for decryption.[2] The encryption key is usually published (the "public key"), while the decryption key is held only by one individual (the "private key"). The two keys are mathematically related (which is why data encrypted with one can be decrypted by the other), but if the scheme is properly implemented, it is thought to be effectively impossible to compute the private key in any reasonable amount of time based only on knowledge of the public key.

Because asymmetric encryption is generally slower than symmetric encryption, most schemes that use asymmetric encryption use a hybrid form. In one common hybrid, the sender symmetrically encrypts her data with a new key, and then encrypts the new key itself asymmetrically with the recipient's public key.[3] The recipient then asymmetrically decrypts the new key, and then can use that key to decrypt the data.

c. Message integrity.

Modern forms of encryption also include message integrity protection, which aims to ensure that the ciphertext (and therefore the cleartext) has not been tampered with. These message integrity mechanisms are relevant both for data at rest (to ensure that the data

[1] Symmetric encryption schemes include AES, DES, RC4, Salsa, and ChaCha.

[2] Asymmetric encryption schemes include RSA, DSA, and Elliptic Curve Cryptography.

[3] Common hybrid schemes include OpenPGP and CMS email encryption, and some forms of Transport Layer Security.

- Checking email through a webmail service like Gmail or Yahoo.
- Online banking and other financial transactions.
- Using a social network like Facebook to talk to friends and family.
- Purchasing goods and services.
- Blogging (e.g., Wordpress) or micro-blogging (e.g., Twitter) to provide public information.
- Communicating with physicians and other medical personnel.
- Online text, audio, and video chat, such as Firefox Hello.
- Using a search engine like Google, Yahoo, or Bing.
- Browsing videos on common video-hosting sites like YouTube.

While many online newspapers and magazines have not yet switched to HTTPS websites, they are moving in that direction, with a coordinated push to finish by the end of 2015.[5]

Beyond web browsing, the use of encryption is widespread and growing. Businesses use

( )-33.7(ha)11.cehc(s)y-7.4(3(d.3(c-0.05)]T0.2 0 Ts-0.014 Tc 0 Tw 1.8[(wh(g)(-7.4)(-0.316(4(p)-0.07)-33.7(e)3(2(e-6(4)3)17.0(,t)-12 14-2(0

Businesses and governments use encrypted storage for sensitive data, to minimize the damage done when information is accidentally leaked.[9]

System administrators (people who maintain computers and networks) use encryption when connecting to the networks that they administer to ensure that their activity cannot be spied upon or interfered with.[10]

Journalists use encrypted email, encrypted chat, and encrypted document-submission systems to talk to sources, editors, and each other.[11]

Software engineers use encryption to communicate with each other to coordinate fixes to sensitive problems.[12]

Encryption is in widespread and rising use across all sectors of society.

query and related session inf

information that is often detailed enough to uniquely identify individuals.[18] One can avoid leaving linkable traces on the Internet by using throwaway computer accounts (and changing them frequently), and by carefully auditing and configuring the software, protocols, and services used.[19]

The most popular online anonymizing tool today is Tor (The Onion Router).[20] Tor assists users who wish to hide their network location by encapsulating their traffic in three layers of encryption and routing that traffic through a series of relays. Those relays do not retain activity logs, and they successively remove the layers of encryption added to the traffic at the outset, so that no single relay can connect the source and destination of the network traffic. While even this sophisticated approach does not guarantee an2(he)-44.(a)11.7356(t)A(s)-14nty

Absent encryption, all networked communications are fundamentally insecure. Anyone with access to the servers that store our data or the networks that transmit it would be able to intercept any communication, tamper with it, or delete it altogether. That fact poses a critical threat to the security of us all in our use of the Internet to store and send our most military systems.[34] These failures can have serious consequences for governments, corporations, journalists, medical providers, law firms, and private citizens alike.

A. Encryption is a basic requirement for security in the digital age.

Cybersecurity broadly encompasses the integrity and confidentiality of stored information and of information in transit over communications networks. Modern, strong encryption is one of the only mechanisms we have to protect these information systems and the social structures that rely on them.

That encryption is essential to this task is well understood within the technical community. Nearly two decades ago, the Internet Architecture Board ("IAB") and the Internet Engineering Steering Group ("IESG") wrote:

> The IAB and IESG would like to encourage policies that allow ready access to uniform strong cryptographic technology for all Internet users in all countries. . . . The Internet is becoming the predominant vehicle for electronic commerce and information exchange. It is essential that the support structure for these activities can be trusted.[35]

A

B. Government proposals to weaken encryption would make everyone's communications and private data less secure.

We have recently heard calls from national governments, including the United States,[44] United Kingdom,[45] and China,[46] demanding "backdoor" mechanisms that would guarantee government access to encrypted communications and data. These mechanisms would likely rely either on key escrow (where the cryptographic keys in any system are duplicated and stored with a third party who can turn them over to law enforcement) or hop-by-hop encryption (where a communications intermediary is able to see the cleartext of any communication and hand it over to law enforcement). Some governments have also tried to weaken cryptographic mechanisms in secret. For example, it is now widely reported that the U.S. National Security Agency introduced, standardized, and encouraged private industry to deploy cryptographic technology that was deliberately weakened.[47]

If adopted, these backdoor measures would undermine the security of the Internet for everyone. Creating backdoor channels of any sort, whether for lawful interception or otherwise, weakens the cybersecurity of the system as a whole. Backdoors are points of weakness that can be exploited not only by law-abiding governments but by rival nation states, repressive regimes, criminals, and others.

The risk of such exploitation is not theoretical. For example, in 2004 and 2005, the mobile phones of dozens of members of the Greek government were spied upon by an unknown adversary who exploited a backdoor intended for law enforcement.[48] And in 2009, Google

ssl.html; Brian Naylor,

servers were breached by Chinese hackers who gained access to a sensitive database with years' worth of information about the U.S. government's surveillance targets.[49]

From an engineering perspective, this risk is also well known. The IAB and IESG commented on deliberately weakened cryptosystems:

> Systems that are breakable by one country will be breakable by others, possibly unfriendly ones. Large corporations and even criminal enterprises have the resources to break many cryptosystems.[50]

And the Internet Engineering Taskav9.3(ne)-446end154(r)-33e3(o)22d( )Tj2H(46)4EÁÀÑ[)1%6,QG²cRedA$d effort, police forces can now determine a suspect's exact location over a period of months, his every confederate, and every other digital fingerprint he leaves when interacting with technology. Federal, state, and local law-enforcement authorities in the United States have eagerly embraced these unprecedented surveillance capabilities.[53] The security that encryption provides must be judged not in a vacuum, but in the context of the pervasive had their private data compromised. Major companies have endured unprecedented intrusions into their systems.[59] And even the government has seen sensitive military information stolen.[60] Virtually every high-level intelligence official in the United States has identified cyberattacks as the most serious threat to the nation's security.[61]

Strong encryption is our first line of defense against that threat. Weakening that encryption would make us all—private citizens and companies alike—more vulnerable to attack. Backdoor access may make law enforcement more efficient, (e)66.3255.6(l).3(en33.7(e)-4)-7.3(d) members of the congress and their families. John and Abigail Adams famously used Lovell's ciphers to encrypt their personal correspondence.[67] Other early encryptors included George Washington, James Monroe, Alexander Hamilton, Aaron Burr, and John Jay, the first Chief Justice of the U.S. Supreme Court.[68]

The role of anonymity in founding-era America was, if anything, even more pronounced: "Our history as a republic was shaped by essays written by anonymous authors."[69] Many of the early American statesmen who debated the principles upon which our country was founded did so behind a veil of anonymity. Indeed, the influential Federalist Papers were published under fictitious names, such as Publius, Americanus, and Caesar.[70] For these "Framers and their contemporaries, anonymity was the deciding factor between whether their writings would produce a social exchange or a personal beating."[71]

The use of encryption and anonymity in the United States as enablers of free expression continues to this day, all the more so since the revelations by Edward Snowden that the National Security Agency is engaging in mass surveillance of innocent individuals around the world.[72]

Tdagleeind t(y)-7.4(8]TJ-0.0(8]T 04 Tc 0 Tw 5.ir.3(ns0 BDC 0067 T Tw 4.533 0 Td8]TJ-0.096 Tc -0.111 Tw 0.24 Tdb24 T.7(lit)55y 21)14.7(-22.o4(s)11.7m24 T4
Nes344a4(x)-7.3,1.4(ec)44(f1 Tc -07)Tc 0w -35.53[2j wonals ad sost(7(s)-14.7(t)-222(e)-2443(m)11.3(i)-2(-4434(6(1)-(3-53(i)3(i)-2 Td[(N)4(a)11.7(nc)3s)e)-44.4(s)]TJ F

matters with journalists, impeding even the everyday but no-less-essential reporting on government ac dissidents or disfavored websites for suppression. China is notorious for such strategies.[84]