Editors: Peter Gutmann, pgut001@cs.auckland.ac.nz | David Naccache, david.naccache@ens.fr | Charles C. Palmer, ccpalmer@us.ibm.com

Freedom of Encryption

Aisling Connolly | École Normale Supérieure

The year is 1943. You need a key. Deciding to keep it simple, you press A, a rotor turns, you take some paper and write K. Press B, write Q. Press C, write G. Again, press A, then B, then C. Write R, N, J. Next, you can begin communication, press W, write D and continue; press E, T, T, E, R, B, E, R, I, C, H, T, write OAJKXTQHETTI. You have your message. Move to your radio and transmit KQGRNJDOAJKXTQHETTI … and you've sent your first encrypted weather report. Does the thought ever arise in your mind as to whether or not it is dishonest to scramble your message? You do this for the sake of national security, for strategy in time of war, for your nation. You need ask no questions; this is your duty.

We jump to 1970. The height of the post-war, Golden Age of Capitalism. Electronic fund transfers (EFTs) are rampant, and the number of issued credit cards surpasses 1 million in the United States. The world's economy is booming. Life is sweet.

It's 1977. Recovering from the 1973–75 recession, you are more skeptical about EFTs. Data protection laws surrounding the collection of payment information are passed. You need more secure systems and welcome the development of DES. But to use it is no mean feat. What was once an instrument solely used for military advantage, encryption is now commercially required due to post-recession insecurities and the growth of electronic and computing industries, and is allowed only through the granting of special licenses.

Let's move to 1991. You possess your own Personal Computer. Imagine that! For the first time, you see the ability to encrypt moving into the hands of the citizen. This yields excitement, but also, it is immediately obvious that this will cause some consternation. On the one hand, the First Amendment of the US Constitution strongly protects freedom of speech and expression, which—in a roundabout way—means that cryptography within the US cannot be controlled. On the other hand, cryptography remains on the US Munitions List, meaning that its export is still heavily regulated.

The next decade sees some of the bloodiest years of the Crypto Wars. With global connection to the Internet, pressure mounts on the US government to loosen the laws surrounding the export of software. The battles are fought in court, and in 1996, encryption software is removed from the Munitions List. By the turn of the century, rules surrounding the export of commercial and open source software containing cryptography are greatly simplified, restrictions on keys are lifted, backdoors are prohibited, and you, the citizen, feel that progress is underway.

Fast-forward to June 2013. You sit happily tip-tapping on your smartphone, sharing Doge memes and giggling over screaming goats,

Copublished by the IEEE Computer and Reliability Societies

before moving on to check the news. You learn that the US government has forced Verizon to hand over the phone records of millions of Americans. It's not such a nice story. Over the coming days you see more articles of a similar vein. You discover the NSA's direct access to data held by all your beloved Internet giants. You learn of secret programs and backdoors, and within months, you come to terms with the fact that you live in a quasi-surveillance state. This is a grave situation, and once again, as you did two decades ago, you find yourself debating the same disparity between individual privacy and state security.

Between then and now. The debate raged on and the disparity still exists. Several nations have the desire to forbid encryption, to keep it as a military tool, to stifle progression, to retain control, and to undermine democracy. But there has also been much progress. Within the coming year, the EU will put two new directives into place: the GDPR (General Data Protection Regulation) and the ePrivacy directive. They expand and solidify the points set out in the Charter of Fundamental Rights of the European Union and the Treaty on the Functioning of the European Union, which state that EU citizens have the right to privacy both online and offline. They insist that in order to maintain security of the individual while ensuring compliance with the regulation, appropriate measures (such as encryption) must be used. The regulations cover the collection, storage, processing, and deletion of personally identifiable information (PII) and personal communications. The regulation applies to the handling of EU citizens' PII irrespective of the location of the organization handling the data.

The United Nations Human Rights Council and the General Assembly have also specified the necessity for encryption to ensure the right to privacy in the digital age, building their argument by paying particular focus to the dangers faced by journalists. The UN[1]

> *[e]mphasizes that, in the digital age, encryption and anonymity tools have become vital for many journalists to exercise freely their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use of such technologies, with any restrictions thereon complying with States' obligations under international human rights law.*

These are simply two examples of many that build upon the arguments of yore. However strong were the efforts made by the privacy advocates in the 90s, they were very few voices. Now, with technology in every inch of our lives, with the increased media attention due to the Snowden revelations, high-profile court cases, and freer flowing information, citizens are much more aware of the consequences of not using encryption. This time around, there are many voices.

And so here we are. You have come a long way since your button-pressing days on the Enigma. You've seen four world recessions, men walking on the moon, the fall of the Berlin Wall, and some moves toward equality. You've danced to records, to cassette tapes, to mp3s, and now to Spotify. You must be tired. But you cannot sit yet! If I ask you to send me an encrypted email, right here and now, can you do it? If I ask you to remove any records of me, to grant my request to be forgotten, is it easy? If I want to travel, to meet people in the world, will you stop me at the border? Will you question me and demand my passwords? If I want to talk, to exercise a curiosity, to learn and teach and spread information, but without prying eyes, will you let me? Ultimately, all I'm asking is to exercise a right. Is it possible?

Until the answer to all of these questions is a definitive *Yes*, then I'm afraid we still have some work to do. ■

Reference

1. "The Safety of Journalists," UN Human Rights Council, A/HRC/RES/33/2, 6 Oct 2016; http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/RES/33/2&Lang=E.

Aisling Connolly is a PhD candidate at the École Normale Supérieure. Contact her at aisling.connolly@ens.fr.