The encryption dustup

Our regular expert columnist **Annie Searle** takes a look at the implications of data protection laws in relation to the Apple encryption case. What does this mean for the detection and prevention of criminal activity – and our right to privacy?

Though the US Department of Justice withdrew its request of Apple, Inc. on March 21, there is no doubt that it, or some other international government agency, will be back to request that a technology provider creates a back door into its encrypted software so the government might read the content on a suspect digital device. Legislation to compel technology companies is already under discussion in both England and France. In France's Digital Republic amendment: "Manufacturers of IT equipment – phones, tablets, computers – are gradually moving toward individual encryption of devices out of a desire to protect their users' personal data…This move is virtuous for protecting personal data. However, it has a downside when faced with the need for the protection and security of the state."

In the proposed French legislation, which has been on the table since earlier terrorist attacks in Paris, companies that do not comply could face up to five years in prison and a roughly US$400,000 fine. [Joshua Eaton, *"With or without evidence, terrorism fuels combustible encryption debate,"* Christian Science Monitor, March 29, 2016.] In the UK, prime minister David Cameron has asked for a ban on encrypted applications that do not offer a back door to law enforcement authorities with a warrant. Undoubtedly, the desire to move such legislation forward will become more intense after recent horrific bombings in Brussels, Bagdad and Lahore. Despite the fact most reports indicate the terrorists in Brussels were using disposable phones and text messages, not an encrypted application like WhatsApp, relationships between governments and the private sector are likely to become more strained as we go forward. It is worth also noting that the failure to find any messaging by terrorists does not automatically mean there must have been encrypted messages, no matter what the current political climate in these three countries might suggest.

The European Commission is working to further refine data protection laws in the European Union, but as they stand, those laws are far more definitive than the Bill of Rights which privacy advocates in the US stand on, which could generally be summarised as the privacy of beliefs, speech and the press (First Amendment); privacy of the home against demands that it be used to house soldiers (Third Amendment); the privacy of the person and possessions as against unreasonable searches, which includes both the evidence of "probable cause" and the use of a warrant (Fourth Amendment); and the Fifth Amendment's privilege against self-incrimination, which provides protection for the privacy of personal information.

In the motion to vacate the government's order, filed by Apple in late February, Apple took the following position with respect to being ordered to write code that would break encryption: "This amounts to compelled speech and viewpoint discrimination in violation of the First Amendment…Under well-settled law, computer code is treated as speech within the meaning of the First Amendment…The Supreme Court has made clear that where, as here, the government seeks to compel speech, such actions trigger First Amendment protections."

Apple also argued: "In addition to violating the First Amendment, the government's requested order, by conscripting a private party with an extraordinarily attenuated connection to the crime to do the government's bidding in a way that is statutorily unauthorised, highly burdensome and contrary to the party's core principles, violates Apple's substantive due process right to be free from 'arbitrary deprivation of [its] liberty by government.'"

We will see these arguments made again, on both sides of the ocean, in legislative chambers and in the press. Apple points out that "examples abound of society opting not to pay the price for increased and more efficient enforcement of criminal laws," which brings us full circle back to Justice Scalia's point that the defence of privacy will sometimes mean criminals are not caught.

Clearly technology has created useful tools for law enforcement over the past several centuries. But the tools were not necessarily created for law enforcement. Cameras were created to record life and events, though some thought them at the time to be an unreasonable violation of privacy. The telephone led not only to streamlined communications but eventually to wiretaps of the highest fidelity. Mobile phone towers/sites created a range of peripheral products, including the StingRay device now quietly used by a wide variety of law enforcement agencies. As devices got smaller and more portable, the ability to retain vast amounts of information grew. In the US, the Supreme Court ruled not long ago that a warrant is required to search a smartphone, just like it is required to search a computer. Both pieces of technology contain not only our email, or our contacts, but also photos we may wish to keep private and messages created out of convenience with an assumption we are using a secure device. Apple and other manufacturers have moved to encrypt our data for us so they are not responsible for it, especially so (given what we know from Edward Snowden's release of classified documents) the government can no longer request our information from them, with or without a warrant. That is what is at the heart of this issue. Operational risks abound, both from the privacy side and in terms of citizens' security, particularly in our ability to live our lives without fear in public places. I would rather see law enforcement acquire better predictive tools than watch them compel global technology companies to deliberately build in back doors to systems or applications we purchase because we believe they are secure. No matter how many attacks we suffer, this issue is not going away, neither in America nor Europe. TRU

"There is nothing new in the realisation that criminality of a few in order to protect the privacy of us all." **US Supreme Court Justice Antonin Scalia, 1987**

Apple and other manufacturers have moved to encrypt our data for us so they are not responsible for it

THE AUTHOR

Annie Searle

Annie Searle is a faculty lecturer at the University of Washington's Information School, where she teaches courses she designed on operational risk, ethics, policy and law as relevant to information technology. She is also principal of Annie Searle & Associates LLC, engaged in research and consulting through the ASA Institute of Risk and Innovation.