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?


“"There is nothing new in the realisation that criminality of a few in order to protect 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.

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

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 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?

There is nothing new in the realisation that criminality of a few in order to protect the Constitution sometimes insulates the privacy of us all.”

US Supreme Court Justice Antonin Scalia, 1987