Privacy, Encryption and Counter-Terrorism

Miller, S.R.M.; Bossomaier, Terry

DOI
10.1007/978-3-030-90221-6_9

Publication date
2021

Document Version
Final published version

Published in
Counter-Terrorism, Ethics and Technology

Citation (APA)
Miller, S. R. M., & Bossomaier, T. (2021). Privacy, Encryption and Counter-Terrorism. In A. Henschke, A. Reed, S. Robbins, & S. Miller (Eds.), *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism* (pp. 139-154). (Advanced Sciences and Technologies for Security Applications). Springer. https://doi.org/10.1007/978-3-030-90221-6_9

Privacy, Encryption and Counter-Terrorism

Seumas Miller and Terry Bossomaier

Abstract Privacy is an important moral right but so is security, including security from terrorist attacks. Encryption protects privacy rights but also affords protection to terrorists and impedes legitimate counter-terrorist operations. This chapter analyses this ethical dilemma.

It is agreed on all sides that there is an important right to privacy, but that security is also important and, in particular, security from terrorist attacks. However, security requirements dictate that privacy rights be infringed at times, e.g. in the case of intercepting emails or phone conversations between terrorists. Moreover, encryption is obviously a good thing since it protects privacy, but potentially problematic if it unreasonably impedes legitimate counter-terrorism operations. The ethical dilemma in this area is exemplified by the following two relatively recent events.

Firstly, there was the conflict between Apple and the FBI [7, 22]. In December 2015, Syed Farook killed 14 people in San Bernardino [4, 26]. The FBI suspected that his phone may have contained information which could implicate others involved in the planning of the attack, or in possible future attacks. However, an Apple iPhone allows only 10 attempts to unlock the phone via its four-digit password before the phone is wiped. Apple refused the FBI request to remove the 10 attempts limit. Ultimately Apple did not have to back down, since a third party succeeded in cracking the phone (including, conceivably, by bypassing or shutting down the auto-erase feature by some means).

Secondly, in mid-2020, Operation Venetic in the UK and coordinated operations in Europe made news when very large criminal networks in the UK and in Europe were destroyed as a result of access to their supposedly secure EncroChat mobile

S. Miller (✉) · T. Bossomaier
Charles Sturt University, Canberra, Australia
e-mail: semiller@csu.edu.au

S. Miller
TU Delft, Delft, Netherlands

University of Oxford, Oxford, England

A. Henschke et al. (eds.), *Counter-Terrorism, Ethics and Technology*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-90221-6_9

phones. Joseph Cox in a thorough article on Vice Motherboard reported that in the Netherlands alone, "the investigation has so far led to the arrest of more than 100 suspects, the seizure of drugs (more than 8000 kilo cocaine and 1200 kilo crystal meth), the dismantling of 19 synthetic drugs labs, the seizure of dozens of (automatic) fire weapons, expensive watches and 25 cars, including vehicles with hidden compartments, and almost EUR 20 million in cash" [5]. In the UK, over 700 arrests—including of crime bosses—have been made, and two tons of drugs (worth over £100 million) have been seized [28]. The phone, which was basically a customised Android phone, provided end-to-end encryption, i.e. email, text messages and voice calls are encrypted on the phone and not decrypted until they reach the destination phone. It is thought the phone was not decrypted but rather hacked into, since malware was apparently found on the EncroChat device itself, meaning that it could potentially read the messages written and stored on the device before they were encrypted and sent over the internet (see Sect. 2). While Operation Venetic concerned criminal organisations primarily engaged in drug dealing, money-laundering, weapons distribution and murder of rival criminals, phones with end-to-end encryption (see Sect. 2) are known to be widely used by terrorists, thus this law enforcement achievement is highly germane to counter-terrorism operations.

These two events graphically illustrate the importance of encryption in law enforcement and in counter-terrorism, in particular. On the one hand, encryption provides privacy protection to ordinary citizens, confidentiality protection to legitimate businesses and, for that matter, confidentiality to police and other security agencies engaged in crime-fighting and counter-terrorism. On the other hand, encryption also affords protection to drug cartels, human traffickers and, of particular interest here, terrorist organizations.

To address this ethical question, we undertake three main tasks. Firstly, we offer an analysis of the nature and moral significance of privacy, including its relationship to confidentiality, autonomy and security, in the context of the counter-terrorism responses of liberal democratic states. Secondly, we provide a description of relevant cryptographic technologies. One focus here will be on WhatsApp, an open architecture, in the sense of being described in a white paper,[1] but not meeting the open-source criterion discussed below, for which we can describe key exchange structure. We explain how the keys work, with minimal mathematics, and the challenges they present to security agencies. By describing the technical issues in some detail, we show how it is that high level end-to-end encryption is, in effect, invulnerable to decryption but also how devices that use such encryption are, nevertheless, vulnerable by virtue of their use of passwords and the possibility of being hacked and the insertion of malware. This section is of particular importance, given the central role this technology has come to play in terrorism and counter-terrorism and given, also, the lack of understanding of the actual powers and limitations of this technology due to its highly technical nature. Our third main task in this article is to provide a discussion of the privacy rights and security needs in relation to encryption in the overall context of the counter-terrorism policies of liberal democratic states.

[1] https://www.whatsapp.com/security.

1 Privacy/Confidentiality, Autonomy and Security

The notion of privacy has proven difficult to adequately explicate [6, 9, 12, 16, 18, 24, 31, 34]. Nevertheless, there are a number of general points that can be made. First, privacy is a right that people have in relation to other persons and organisations with respect to: (a) the possession of personal information about themselves by other persons and by organisations, e.g. data stored in telecommunication company, technology company, or government databases, (b) the observation/perceiving of themselves—including of their movements, relationships and so on—by other persons, e.g. via CCTV or mapping metadata to determine geolocation history; (c) the interception of their communications, e.g. phone conversations, emails.

Second, the right to privacy is closely related to the more fundamental moral value of autonomy. Roughly speaking, the notion of privacy delimits an informational and observational 'space' i.e. the private sphere. However, the right to autonomy consists of a right to decide what to think and do and, of relevance here, the right to control the private sphere and, therefore, to decide *whom to exclude and whom not to exclude* from it. So, the right to privacy consists of the right to exclude organisations and other individuals (the right to autonomy) both from personal information and facial images, and from observation and monitoring (the private sphere). Naturally, the right to privacy is not absolute; it can be overridden. Moreover, its precise boundaries are unclear; a person does not have a right not to be casually observed in a public space but, arguably, has a right not to have their movements tracked via their smartphone, albeit this right can be overridden under certain circumstances, e.g. if they are terrorism suspects.

Third, a degree of privacy is necessary simply in order for people to pursue their personal projects, whatever those projects might be. For one thing, reflection is necessary for planning, and reflection requires a degree of freedom from the distracting intrusions, including intrusive surveillance, of others. For another, knowledge of someone else's plans can lead to those plans being thwarted (e.g. if one's political rivals can track one's movements and interactions then they can come to know one's plans in advance of their implementation), or otherwise compromised, (e.g. if who citizens vote for is not protected by a secret ballot, including a prohibition on cameras in private voting booths, then democracy can be compromised). *Autonomy*—including the exercise of autonomy in the public sphere—requires a measure of privacy.

Thus far we have described privacy and autonomy, considered as the rights of a *single* individual. However, it is important to consider the implications of the infringement, indeed violation, of the privacy and autonomy rights of the whole citizenry by the state (and/or other powerful institutional actors, such as corporations). Such violations on a large scale can lead to a power imbalance between the state and the citizenry and, thereby, undermine liberal democracy itself. The surveillance system imposed on the Uighurs in China, incorporating a full range of technologies including phone metadata, facial recognition, DNA, etc., graphically illustrates the

risks attached to large scale violations of privacy and related autonomy rights if governments use them in a discriminatory manner [8, 11, 17, 20].

In light of the above analysis of privacy, and especially its close relationship to autonomy, we are entitled to conclude that some form of privacy is a constitutive human good. As such, infringements of privacy ought to be avoided. That said, as mentioned above, privacy can reasonably be overridden by security considerations under some circumstances, such as when lives are at risk. After all, the right to life is, in general, a weightier moral right than the right to privacy.

Individual privacy is sometimes confused with anonymity, but these are distinct notions. Anonymity is preserved when a person's identity in one context is not known in another. Anonymity can be a means to privacy or to avoid harm to oneself e.g. reputational damage. Indeed, anonymity is vital in some situations, for example in the case of an undercover operative whose real identity might be revealed to the criminal organisation he has infiltrated by using facial recognition technology to search billions of facial images on the Internet, social media and elsewhere that were originally created some years earlier when he worked as a uniformed police officer. Such examples demonstrate that anonymity is sometimes an instrumental good. But they do not demonstrate that it is a constitutive human good. In this respect anonymity is quite different from privacy.

The sphere of individual privacy can be widened to include other individuals who stand in a professional relationship to the first individual, for example, a person's doctor. Moreover, morally legitimate institutional processes give rise to confidentiality requirements with respect to information. For instance, law enforcement operations give rise to stringent confidentiality requirements, given what is often at stake, e.g. the outcome of important investigations that could be compromised by exposure or, as mentioned above, the risk to an undercover operative if their identity is revealed [21]. At least in the case of security agencies, such as police, military and intelligence agencies, a degree of compliance with principles of confidentiality is a constitutive institutional good in the sense that security agencies could not successfully operate without a high degree of confidentiality.

Confidentiality is often referred to as informational *security*. So, confidentiality is a species of security. Moreover, confidentiality is, as we saw above, often based on privacy, e.g. the confidentiality of personal information. Accordingly, not only is privacy not necessarily in conflict with security: privacy quite often depends on security. On the other hand, the integration or interlinking of databases of confidential information is potentially problematic from a privacy and autonomy perspective, as the example of the surveillance system in China described above demonstrates.

Another related notion of interest to us here is secrecy [3]. Secret information is not necessarily challenged by the moral right to privacy or by the principle of confidentiality. For unlike privacy and confidentiality, secrecy is a morally neutral or even pejorative notion. Secrecy is at home in contexts of conflict and fierce competition, for example wars, organised criminality and market-based companies. More generally, secrecy is at home in contexts of security. However, high levels of secrecy can mask incompetence, corruption, illegality and human rights abuses, for example in authoritarian regimes. Also, as mentioned above, even in liberal democracies there is

the risk that if the use of the database is not closely monitored and transparent then it will be used for unintended purposes such as surveillance, and, thereby, enable function creep. Accordingly, in contrast with confidentiality, secrecy is not a constitutive institutional good.

We have distinguished privacy, autonomy, anonymity, confidentiality and secrecy, and argued that whereas privacy is a constitutive human good—in part by virtue of its relation to autonomy—and confidentiality a constitutive institutional good, neither anonymity nor secrecy are constitutive goods [20]. Given the close relationships between privacy and confidentiality, on the one hand, and between confidentiality and security, on the other hand, the sharp contrast often drawn between privacy and security does not necessarily obtain.

The notion of security is somewhat vague. Sometimes it is used to refer to a variety of forms of collective security, for example national security (such as harm to the public from a terrorist attack), community security (such as in the face of disruptions to law and order posed by violent political demonstrations) and biosecurity (such as threats to public health and society caused by COVID-19). At other times it is used to refer to personal physical security.

Aside from questions about the scope of security, (for example the personal, organisational and national levels), security can be distinguished by type. Here a distinction between informational and non-informational security can be helpful. Informational (or data) security, as mentioned above, basically consists in ensuring that personal and other confidential information are protected from unauthorised or otherwise illegitimate access. Encryption (of which more in the following section) plays a key role in ensuring data security. Clearly data security is critical in the face of sustained hacking by state and non-state actors that can compromise privacy and confidentiality. Non-informational security pertains to physical or psychological harm to human beings, damage to physical objects, and certain forms of harm to institutional processes or purposes, for example by means of corruption.

Aside from the scope and types of security there are also various contexts of security. These include crime, counter-terrorism, war, cyberwar, trade ‘wars’ and so on. Moreover, the stringency of privacy rights and confidentiality requirements need to be relativized to context. In wartime, for instance, military intelligence gathering is largely unfettered and the privacy rights of citizens curtailed under emergency powers. By contrast, in domestic law enforcement there is, as we saw above, a strong presumption in favour of the privacy rights of citizens. Moreover, in domestic law enforcement there is likely to be increased accountability when privacy rights are overridden. For instance, police might not be able to sign off on access to personal information; rather a judicial warrant might be required. Counter-terrorism in well-ordered jurisdictions is typically a matter of law enforcement. However, in war zones, such as combating Islamic State in Iraq and Syria, counter-terrorism operations, including intelligence gathering, are military in character [19]. Let us now turn to cryptographic technologies, an understanding of which is necessary if we are to offer a coherent account of the ethical problems in this area.

2 Encryption

Modern computer-based cryptography comes in a number of methodologies, e.g. public/private key (PPK) cryptography. For our purposes here, we first need to distinguish between passwords and keys. A password can be thought of as an access mechanism; a key is used in an encryption algorithm. Passwords are often quite short, e.g. eight characters. Being short, passwords are susceptible to brute force attack; an attack in which every possible combination is tried in succession, until the solution is found. Thus, protection from unauthorised access is often afforded by a mechanism which wipes all content on the device after, say, 10 attempts to find the password, as in the case of the iPhone of the terrorist Farook mentioned above. By contrast, keys are a lot longer—the longer the better—and are sometimes retrieved by user entered passwords. Accordingly, even in the case of encrypted material there is potentially a weak link in the chain, namely, the password; depending, of course, on the strength of the password and how securely it is held, (e.g. not written down and pasted on one's computer!) Note that a password when it is sent over the net, to say a bank website, is encrypted by the web browser, typically using strong keys. Whereas we would think of a password in terms of the number of characters, the length of a key is usually given in bits. A bit is the information in a binary (two option) choice, a logical yes or no. Thus, a bit can be represented as a zero or one and we could write the key as a series of zeroes or ones. Since a character is normally 8 bits we could think of a 2048 bit key as equivalent to 256 characters (i.e. 8×256).

It is important to distinguish encryption of documents and data on a device, such as a phone, from encryption in transmission. The first involves some sort of encryption control, of which a password is the most well-known, but there are other options, such as fingerprint, retinal scan, and so on. Despite ongoing efforts on the part of cyber-security personnel to promote the importance of password protection, people persist in using easy-to-guess passwords, which are thus easy to remember, the name of the dog, house address, favourite fruit, etc. A brute force attack on a password (testing every possibility) requires time proportional to m^n where m is the number of options for a character and n is the number of characters. Thus an 8-character password using alphanumeric characters (the integers 0–9 and the 26 letters of the alphabet in both lower and upper case) gives rise to 62^8 possibilities i.e. 200 trillion—which a desktop computer could run through in a relatively short time. If we use the most widely used mapping of letters, numbers and symbols to bit patterns, i.e. the whole extended ASCII[2] character set of 256 characters, we get 256^8 possibilities, i.e. millions of trillions. So the number of possibilities is a function not only of the length of the password but also of the number of available characters, although, since the number of characters appears in the exponent, increasing the number of characters is usually a more effective way of increasing password strength. However, there

[2] ASCII stands for American Standard Code for Information Interchange. Computers can only understand numbers, so an ASCII code is the numerical representation of a character such as 'a' or '@' or an action of some sort. ASCII was developed a long time ago and now the non-printing characters are rarely used for their original purpose.

needs to be very large numbers of possibilities to defeat even a standard desktop computer. On the other hand, there can be *very* large numbers of possibilities which a standard computer would take decades to run through. Brute force attacks, in which every possibility is tested in sequence or at random, on common standards such as AES would take forever. But encryption may be broken on a much smaller timescale through two mechanisms: the advent of new technology; or new algorithms which test possibilities in some special order or apply some novel filtering. Moore's law, the doubling of computing power every two years has held since 1965 for current silicon. Yet an example of a novel technology is quantum computing, which is rapidly developing at the time of writing, where it has been known since 1999 when Peter Shor's now famous 1999 algorithm demonstrated huge potential speedup from quantum computers for prime factorisation and discrete logarithms [29]. An example of new software attacks came in a series of novel attacks on AES-256, summarised by cryptographer Bruce Schneier[3] *This new attack, by Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir, is much more devastating. It is a completely practical attack against ten-round AES-256—One of our attacks uses… 2^{39} time to recover the complete 256-bit key… where the best previous attack required 2^{120} time.*

Estimating the time for an actual computer to crack a key by brute force obviously depends upon the rapidly growing speed of computers. Nevertheless, MIT physicist Seth Lloyd estimated an upper bound to the speed of a 1 kg laptop based on the laws of physics as they stand today [15]. His ultimate laptop would take about a microsecond to break AES 128. It would take an ultimate computer the size of the Earth about a year to crack AES 256. Needless to say, we don't expect to have ultimate computers any time soon.

If we want to send the document over a public channel we need a good password, obviously, and the recipient needs to have learned this password in some way (such as Diffie Hellman, which we discuss below). However, if we use public private key cryptography (PPK), with, say, a typical key of 2048 bits, 2^{231} possibilities, then the communication is even stronger. If somebody intercepts the document, this is the strength of encryption with which they have to deal. The password stays on the device and is not transmitted. The alternative to encrypting the document and sending it over a public channel, is to use an encrypted channel, such as WhatsApp. Any useful channel has to be end-to-end encrypted, meaning that is encrypted on the source device and not decrypted until it gets to the destination device. To avoid key compromise by some means, systems such as WhatsApp use ephemeral keys, into more detail of which we go below.

It is important to distinguish between the interception of communications in real time and the accessing of stored material, including documents. Stored material, even if encrypted, is susceptible to accessing if the device is retrieved by investigators and its password determined. Real-time interception of, and access to, the content (as opposed to the metadata, e.g. time, date, location, sender and receiver of call) of communications protected by end-to-end encryption will be extraordinarily difficult

[3] https://www.schneier.com/blog/archives/2009/07/another_new_aes.html *Accessed*.

unless the communication is intercepted prior to encryption or after decryption. This is because the required decryption is extraordinarily difficult, absent access to encryption keys. (For more details on this see below). Crucially, the encryption keys used for communications in devices using end-to-end encryption are typically ephemeral; they are only used for a single message transmission and then discarded. Accordingly, since WhatsApp, for instance, uses end-to-end encryption, security agencies cannot usefully wire-tap phones using WhatsApp, since anything they acquired would not be decryptable.

Typically, encryption keys resist brute force attacks by virtue of the vast number of possibilities that would have to be tried in the time period available, e.g. a number of possibilities of such magnitude that it would take even a high-powered computer decades to find the correct one. Thus, the RSA algorithm used in PPK requires two very large prime numbers, p and q, which are multiplied together to produce an even bigger number $N = pq$. Take a number such as 1333. This factorises into 31 times 43, which are both prime numbers. The important thing to know is that as the numbers such as 1333 get bigger, it becomes very difficult to find the constituent primes (31 and 43). The idea is to make N so big, that finding the two prime factors would take an inordinate amount of time. Hence there has been the pressure on governments from law enforcement and security agencies to enforce access to encryption keys.

To allow security agencies to eavesdrop on conversions with WhatsApp and its kin, is rather complicated, owing to the hierarchy of keys of different lifetimes used in the encryption. Thus, let us consider the simpler case of giving security agencies access to private keys, assuming that there are suitable judicial processes to allow access only in case of real need, along the lines already discussed. Storing all these private keys is itself a security risk: they may get leaked, stolen by hackers or just left in unsecured places by defective software due to careless programmers. An alternative is a sort of skeleton private key, sometimes referred to as a backdoor key. The same issue of keeping skeleton key safe applies of course, but there is an additional problem. There is pretty much consensus amongst cryptographers that creating the structure for such backdoor access weakens the encryption, thus making it easier for hackers to break [2, 13, 14].

In the face of this resistance to providing encryption keys to governments, law enforcement's focus has been on finding passwords or on means of attack that do not rely on decryption by virtue of knowing the keys, but rather on bypassing the keys, e.g. by inserting malware into devices as happened in the EncroChat case (described above). There is also, of course, the possibility of legislation, such as exists already in the UK, where a warrant can be obtained to compel a suspect to decrypt a document with prison terms for non-compliance.

Of course, we will not know for some time exactly how EncroChat was compromised, since the security agencies are hardly likely to divulge this information. The consensus seems to be that this was not a defeat of the encryption but the capturing of messages before they were encrypted and sent, through spyware, which had got into the phone. It was most likely downloaded from EncroChat servers, which had themselves been infected, and then infected phones with something quite ordinary, such as a news release or a software update. One common spyware technique is key

logging. Every key pressed by the user is recorded in some place hidden to the user and sent across the internet to the spyware's owner. Most, if not nearly all, phone apps phone home on a regular basis, usually without the user knowing [32].

The principal encrypted voice call and message systems at the moment are: Signal, Telegram, WhatsApp (owned by Facebook) and Facetime (owned by Apple). Let us consider WhatsApp as illustrative. WhatsApp was very popular, even before it was taken over and became part of Facebook infrastructure. It is end-to-end encrypted, the gold standard, which means that it is encrypted by the sender, decrypted by the receiver and not decrypted anywhere along the way. A highly desirable feature of encrypted messaging is that it should be *open source*. Effectively this means anybody, especially cryptography experts, to scrutinise the details of the algorithms and their implementation. WhatsApp was developed from Signal, using the so-called Signal protocol, and Signal is open source. WhatsApp is not. However, despite recent controversy over the sharing of its *metadata* with parent company Facebook, the best available evidence is that it is still end-to-end encrypted. The EFF (Electronic Frontiers Foundation, one of the leading advocates for technology supporting freedom and justice) states in January 2021 that[4] *To be clear: WhatsApp still uses strong end-to-end encryption, and there is no reason to doubt the security of the contents of your messages on WhatsApp.*

Of course, the provider could have a system in which they keep the encryption keys and save the messages, which means that the message could be decrypted by a third party at a later date. As discussed above, law enforcement has supported this since it would be to their advantage. At any rate, to give users confidence in their communications being forever secret, and as we saw above, the app uses ephemeral keys, which are created for a particular message transmission and then discarded. The user's private keys are never sent anywhere and are not known to the provider.

There are basically two approaches to encrypting a document: block ciphers, such as AES, which break the document up into chunks (blocks) and encrypt each individually; and stream ciphers such as RC4 (Rivest Cipher 4, after its inventor), which operate one character at a time.

Today's block ciphers are both very complicated and very secure. The data is broken up into blocks. Each sub-block is individually encrypted using algorithms then combined with other blocks and the process repeated for a dozen or so iterations. The current more secure version is AES256.

Stream ciphers date back to the sixteenth century with the invention of the one-time pad, beloved of espionage stories ever since. The pad is some document, say Tolstoy's book, *War and Peace*. Starting at some agreed place in the book (our spies have to agree on the book and where to start) the message is compared letter by letter with the book and some reversible algorithm is used to go from one to the other. Thus, if the message has a k and the book at the same point has a q, then the algorithm would output, say, a z. Going backwards taking the z in the encrypted document, comparing it with the q in the book spits out k. The algorithm commonly used is XOR. The computational equivalent is the Vernam cipher which combines the characters of a

[4] https://www.eff.org/deeplinks/2021/01/its-business-usual-whatsapp *Accessed*.

document one by one with a random character from the keystream (the letters one by one from the book in our Tolstoy example). The one-time pad and consequently the Vernam Cipher were shown by Claude Shannon to be unbreakable, given that the one-time pad is perfectly random [27]. In the Vernam cipher we use a keystream, which is just a random series of characters. Computer random number generators are now very good at producing very long strings of integers/characters with no relationships between them and no recurring patterns of any kind. But they are only ever pseudo-random. The generator will have control parameters and a starting state, and, if these are replicated, the replica will enable the production of exactly the same sequence. As is obvious, in the pre-digital computing days of cryptography keeping the code book secure was vitally important. Of course, with the advent of keystream (Vernam) ciphers, the code book has been replaced by a random number generator. However, it is now vitally important to keep the details of its parameters and starting state (though not necessarily its algorithm) secure.

An essential point to note here is that cryptographic systems may fail for three reasons: computer power increases allowing a brute force attack (essentially working through every possibility, as mentioned above); the invention of new attack algorithms, or hardware, such as quantum computers; and simply flaws in implementation.

The most effective attacks are not brute force, but exploit some loophole in the cryptography design. Mostly the problems are in software, but occasional a bug appears at the hardware level. This year *The Verge* reported on a particularly nasty vulnerability in Intel chips, which could enable the construction of key loggers, referred to above:

> Security firm Positive Technologies discovered the flaw, and is warning that it could break apart a chain of trust for important technology like silicon-based encryption, hardware authentication, and modern DRM protections. This vulnerability jeopardizes everything Intel has done to build the root of trust and lay a solid security foundation on the company's platforms, explains security researcher Mark Ermolov. [35]

Such hardware vulnerabilities are extremely hard to fix (in the worst case requiring chip replacements) [1]:

> These types of attacks, called Meltdown and Spectre, were no ordinary bugs. At the time it was discovered, Meltdown could hack *all* Intel *x*86 microprocessors and IBM Power processors, as well as some ARM-based processors. Spectre and its many variations added Advanced Micro Devices (AMD) processors to that list. In other words, nearly the whole world of computing was vulnerable… …fixing these vulnerabilities has been no easy job.

Of course, programmers can make errors in implementing cryptographic algorithms. Cryptography is not immune to software bugs.

A fundamental problem in cryptography is agreeing on passwords or encryption keys, using a public channel, where everybody can read the transmissions but cannot infer the password. This is the idea behind a Diffie-Hellman *key exchange* used in PPK and in ECC (elliptical curve cryptography) replied upon by WhatsApp. The following gives a rough idea of how it works.

Xenakis and Zadok want to agree a password. First, they each choose a very large prime number as a private key. Xenakis chooses 43 and Zadok chooses 31.

Now X and Z pick a number, let's say 187. They agree on this over the public channel and again, anybody can know. Now comes the clever trick. X raises 187 to his secret number, 43, getting the very large number.

488865152806014591286861686772706319230312571680272204886482348452897213037526469889220501379640003.

Meanwhile Z does the same with his secret number, 31, getting.

267355918526760594517850396244682696965075500600103129693871671202741630.

X and Z exchange their huge numbers. It doesn't matter if anybody is eavesdropping, since the discrete logarithm problem is hard to solve for them to find either X or Z's secret number. Now each takes the number they receive and exponentiates it with their own secret number. X gets an even bigger number, which would take a page to display. It starts off.

231665580218583671305288093321307899324630293544208947916938366460879672381619542742004634462489560464123889608443987676651933304066297159504611394237176564266553596920948483807064794844917502309225700343433 4.

Z does the same. She takes the big number she gets from X, call it x_1 and computes x_1^{31}. Her number begins.

231665580218583671305288093321307899324630293544208947916938366460879672381619542742004634462489560464123889608443987676651933304066297159504611394237176564266553596920948483807064794844917502309225700343434

and, in fact, they are *exactly* the same. This huge number is now their shared password. To work out this password from the public traffic, the eavesdropper would need to solve a big discrete logarithm problem.

Let us conclude this section by considering the level of security on Apple devices. Apple has two backup options [36].

1. Via Finder/iTunes, you can turn on encrypted backup (it is off by default). If you do so you need to create a password. But there is no way of using the backup if you lose the password. Thus, you must create a password that you'll remember or you must write it down and store it safely, because there's no way to use your backup without this password.
2. Via iCloud (the default and apple preferred option). Now Apple has the encryption keys. It would argue that this is good for users since if they lose the password, Apple can recover it.

However, although Chinese iPhones will retain the security features that can make it all but impossible for anyone, even Apple, to get access to the phone itself, that will not apply to the iCloud accounts [23]. Any information in the iCloud account could be accessible to Chinese authorities who can present Apple with a legal order. Elsewhere the keys are stored by Apple in the US, which means, under a suitable court order in the US courts, Apple could be forced to give up the keys and hence the data on the phone. Now it seems that WhatsApp messages are backed up to the

cloud unencrypted. From their FAQ, WhatsApp chat histories aren't stored on their servers. Media and messages you back up aren't protected by WhatsApp end-to-end encryption while in iCloud. If you've previously backed up your iPhone using iCloud or iTunes, you might be able to retrieve your WhatsApp chats by restoring your iPhone from a previous backup.

In a strange twist, Google, which depends heavily on targeted advertising revenue, and obtains this through massive surveillance of how its users employ its services, nevertheless offers greater personal security than Apple. Data backed up to Google is encrypted by a key, accessed by the phone's pin number or fingerprint etc., and this key is controlled on Googles' servers by a custom chip referred to as Titan. Now, since a pin number is a very weak password, the Titan uses the old maximum number of tries principle (although we do not know how many tries this actually amounts to) [10]. The limited number of incorrect attempts is strictly enforced by a custom Titan firmware that cannot be updated without erasing the contents of the chip. By design, this means that no one (including Google) can access a user's backed-up application data without specifically knowing their passcode.

3 Ethical Analysis

In the light of our conceptual analysis of privacy, confidentiality, autonomy and security, and our descriptive technical account of encryption, we can now offer an ethical analysis of privacy rights and security needs in relation to encryption in the overall context of the counter-terrorism policies of liberal democratic states. Before addressing the specific issues of privacy and encryption in counter-terrorism, a number of general points that bear on this issue and which are extractable from the discussions in Sects. 1 and 2 need to be made.

We have argued that privacy rights, including in respect of smartphone content and metadata, are important, in part because of their close relation to autonomy. However, we also noted that privacy rights are not absolute; they can justifiably be overridden, for instance, in relation to an imminent terrorist attack. Therefore, the strong claim that some privacy advocates are inclined to make, namely, that there is, in effect, an absolute moral right to very strong, i.e. uncrackable, encryption, since it asserts there are no circumstances in which very strong encryption should be impermissible, is not sustainable. This is, of course, not to demonstrate that very strong encryption is morally impermissible under all circumstances. Perhaps, for instance, citizens who live in an authoritarian state are morally justified in possessing devices equipped with very strong encryption. Moreover, even in liberal democracies very strong encryption might be morally permissible if there were other means by which law enforcement agencies could efficiently and effectively investigate and, if justified, charge terror suspects. For instance, if bulk metadata (as opposed to communicative content) in the context of machine learning techniques combined with other methods, such as hacking and insertion of malware was sufficient (as presumably occurred in the EncroChat scenario). On the other hand, bulk metadata collection and, relatedly, integrated databases, are themselves problematic from a privacy perspective.

Although privacy rights can be overridden under some circumstances, notably by law enforcement investigations of serious crimes including terrorism, there is obviously a point where infringements of privacy rights are excessive and unwarranted. Security agencies' ongoing, ready access to the personal data of the entire population would be clearly unacceptable. Moreover, regulation, and associated accountability mechanisms need to be in place to ensure that, for instance, personal information obtained for a legitimate purpose, such as counter-terrorism, can be accessed by law enforcement officers to enable them to detect suspects and protect citizens from being murdered, but not used to identify protesters at a political rally [25].

We have also argued that the sharp contrast between privacy and security cannot be maintained, since security includes informational or data security, i.e. security of personal data and confidentiality in relation to data held by security agencies. Moreover, it is primarily goods that are not essentially informational that ultimately need to be weighed so as to achieve an acceptable moral equilibrium, notably individual autonomy, personal security and institutional integrity.

Moreover, by describing the technical issues in some detail we have shown how it is that high level end-to-end encryption is, in effect, invulnerable to decryption. However, as we have also shown by describing the technical issues in some detail, how devices that use such encryption are, nevertheless, vulnerable by virtue of their use of passwords and the possibility of being hacked and the insertion of malware.

In the light of the above, a number of interconnected ethical issues have come into view. Some of these arise from the expanding use of bulk data collection and surveillance in counter-terrorism operations, especially in the context of interlinkage of databases, data analytics and artificial intelligence. As already mentioned, these developments are relevant to debates surrounding encryption in so far as they provide an advantage to security agencies that might to some extent mitigate the problem of not having access to encrypted communications and documents.

This is not to say that there ought not to be constraints on bulk data collection and analysis. For instance, it is unacceptable for data, including surveillance data, originally and justifiably gathered for one purpose, e.g. taxation or combating a pandemic, to be interlinked with data gathered for another purpose, e.g. counter-terrorism, without appropriate justification. The way metadata use has expanded from initially being used by only a few agencies engaged in counter-terrorism to now being used quite widely by governments in many western countries, is an example of function creep.

Another important development that needs to be kept in mind when adjudicating privacy and encryption issues in counter-terrorism contexts is the blurring of the distinction between the application of the domestic law enforcement and the military combat frameworks in counter-terrorism operations, given that terrorist organisations, such as Al Qaeda and Islamic State operate in war zones as well as in well-ordered jurisdictions. What are the privacy rights of, for instance, those suspected of travelling abroad with the *intention* of becoming foreign terrorist fighters but who are yet to fulfil this intention? Should they be treated as ordinary citizens possessed of

the full array of privacy and other rights who are only potential, and not actual, criminals?[5] Again, what are the privacy rights of those suspected of being foreign terrorist fighters who have returned to their home country? Should they be treated as ordinary citizens possessed of the full array of privacy and other rights albeit, if returnees, citizens suspected of criminality? Or should they be regarded, in effect, as suspected terrorist-combatants and, therefore, suffer a curtailment of their privacy and other rights even in the absence of sufficient evidence to convict them of terrorist offences, e.g. in relation to privacy, the ongoing monitoring of their private communications by domestic security agencies, the retention of their personal data by domestic security agencies, and the disclosure of this data to third parties such as foreign governments and their security agencies [33].

Finally, it should be noted that there is a danger in relation to the technological developments discussed here (e.g. bypassing encryption and the use of integrated bulk databases), as there is in relation to technological developments discussed elsewhere (e.g. the use of facial recognition technology) [30], that various general principles hitherto taken to be constitutive of liberal democracy are gradually undermined, such as the principle that an individual has a right to freedom from criminal investigation or unreasonable monitoring (including accessing of the content of their communications), absent prior evidence of violation by that individual of its laws. In a liberal democratic state, it is generally accepted that the state has no right to seek evidence of wrongdoing on the part of a particular citizen or to engage in selective monitoring of that citizen, if the actions of the citizen in question have not otherwise reasonably raised suspicion of unlawful behaviour and if the citizen has not had a pattern of unlawful past behaviour that justify monitoring. However, this principle is potentially undermined by certain kinds of offender profiling and, specifically, ones in which there is no specific (actual or reasonably suspected) past, imminent or planned crime being investigated. We note that not simply communicative content but also metadata could be used for profiling, risk assessment and monitoring of people who are considered at risk of committing crimes. Moreover, in a liberal democratic state, and related to the above-mentioned principle, there is a general presumption against the state monitoring the citizenry. This presumption can be overridden for specific purposes but only if the monitoring in question is not disproportionate, is necessary or otherwise adequately justified and kept to a minimum, and is subject to appropriate accountability mechanisms.

In this chapter we have performed three main interconnected tasks. First, we have offered an analysis of the nature and moral significance of privacy, including its relationship to confidentiality, autonomy and security, in the context of the counter-terrorism responses of liberal democratic states. Second, we have provided a description of relevant cryptographic technologies. One focus here has been on WhatsApp. Third, we have discussed the privacy rights and security needs in relation to encryption in the overall context of the counter-terrorism policies of liberal democratic states.

[5] Although in some jurisdictions, such as Australia, travelling to Syria and other zones of armed conflict is in and of itself a crime. See Section 119.2 of the Criminal Code of Australia.

Acknowledgements I, Seumas Miller (co-editor), would like to thank for the funding from the ERC Advanced Project on Collective Responsibility and Counter-terrorism (of which I am the Principal Investigator).

References

1. Abu-Ghazaleh N, Ponomarev D, Evtyushkin D (2019) How the spectre and meltdown hacks really worked. IEEE Spectrum. https://spectrum.ieee.org/computing/hardware/how-the-spectre-and-meltdown-hacks-really-worked. Accessed 24 Sept 2020
2. Benaloh J (2018) What if responsible encryption back-doors were possible? Lawfare. https://www.lawfareblog.com/what-if-responsible-encryption-back-doors-were-possible. Accessed 29 Sept 2020
3. Bok S (1982) Secrets: on the ethics of concealment and revelation. Pantheon Books, New York
4. Botelho G, Ellis R (2015) San Bernardino shooting investigated as 'act of terrorism'. CNN. https://edition.cnn.com/2015/12/04/us/san-bernardino-shooting/index.html. Accessed 5 May 2021
5. Cox J (2020) How police secretly took over a global phone network for organized crime. Vice Motherboard. https://www.vice.com/en/article/3aza95/how-police-took-over-encrochat-hacked. Accessed 2 July 2020
6. Fried C (1969) Privacy. Yale Law J 77(3):475–493
7. Grossman L (2016) Inside Apple CEO Tim Cook's fight with the FBI. Time. https://time.com/4262480/tim-cook-apple-fbi-2/. Accessed 5 May 2021
8. Henschke A (2017) Ethics in an age of surveillance: virtual identities and personal information. Cambridge University Press, New York
9. Inness JC (1992) Privacy, intimacy, and isolation. Oxford University Press, New York
10. Jonnalagadda H (2020) Apple may have ditched encrypted backups, but Google hasn't. Android Central. https://www.androidcentral.com/apple-may-have-ditched-encrypted-backups-google-hasnt. Accessed 28 Sept 2020
11. Kleinig J, Mameli P, Miller S, Salane D, Schwartz A (2011) Security and privacy: global standards for ethical identity management in contemporary liberal democratic states. ANU Press, Canberra
12. Koops B-J, Newell BC, Timan T, Škorvánek I, Chokrevski T, Galič M (2016) A typology of privacy. Univ Pennsylvania J Int Law 38(2):483–575
13. Landau S (2018) Exceptional access: the devil is in the details. Lawfare. https://www.lawfareblog.com/exceptional-access-devil-details-0. Accessed 29 Sept 2020
14. Landau S (2020) If we build it (they will break in). Lawfare. https://www.lawfareblog.com/if-we-build-it-they-will-break. Accessed 29 Sept 2020
15. Lloyd S (2000) Ultimate physical limits to computation. Nature 406(6799):1047–54
16. Lucas GR (2013) Privacy, anonymity, and cyber security. Amsterdam Law Forum 5(2):107–114. https://doi.org/10.37974/ALF.253
17. Macnish K (2018) Government surveillance and why defining privacy matters in a post-Snowden world. J Appl Philos 35(2):417–432. https://doi.org/10.1111/japp.12219
18. Matthews S (2010) Anonymity and the social self. Am Philos Q 47(4):351–363
19. Miller S, Feltes J, Henschke A (2021) Counter-terrorism: the ethical issues. Edward Elgar, London
20. Miller S, Walsh P (2016) NSA, snowden and the ethics and accountability of intelligence gathering. In: Galliott J, Reed W (eds) Ethics and the future of spying: technology, intelligence collection and national security. Routledge, London, pp 193–204
21. Miller S, Gordon I (2014) Investigative ethics: ethics for police detectives and criminal investigators. Wiley-Blackwell

22. Nakashima E (2016) Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks. The Washington Post. https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html. Accessed 5 May 2021
23. Nellis S, Cadell C (2018) Apple moves to store iCloud keys in China, raising human rights fears. Reuters. https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060. Accessed 28 Sept 2020
24. Nissenbaum H (2009) Privacy in context: technology, policy, and the integrity of social life. Stanford Law Books
25. Robbins S (2021) Bulk metadata collection and the right to privacy. In: Miller S, Feltes J, Henscke A (eds) Counter-terrorism: the ethical issues. Edward Elgar, London
26. Schmidt MS, Pérez-Peña R (2015) F.B.I. Treating San Bernardino attack as terrorism case. New York Times. https://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html. Accessed 5 May 2021
27. Shannon CE (1945) A mathematical theory of cryptography. Index PO. 4, Memorandum for file, case 20878, MM 45-110-92
28. Shaw D (2020) Hundreds arrested as crime chat network cracked. BBC News. https://www.bbc.com/news/uk-53263310. Accessed 2 July 2020
29. Shor PW (1999) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev 41(2):303–332
30. Smith M, Miller S (2021) The ethical application of biometric facial recognition technology. AI Soc. https://doi.org/10.1007/s00146-021-01199-9
31. Solove D (2008) Understanding privacy. Harvard University Press, Harvard
32. Swinhoe D (2018) What is a keylogger? How attackers can monitor everything you type. CSO. https://www.csoonline.com/article/3326304/what-is-a-keylogger-how-attackers-can-monitor-everything-you-type.html. Accessed: 29 Sept 2020
33. UNSC (2015) Gaps in the use of advance passenger information and recommendations for expanding its use to stem the flow of foreign terrorist fighters, 26 May 2015, S/2015/377, para 44
34. Warren SD, Brandeis LD (1890) The right to privacy. Harv Law Rev 4(5):193–220
35. Warren T (2020) A major new Intel processor flaw could defeat encryption and DRM protections. The Verge. https://www.theverge.com/2020/3/6/21167782/intel-processor-flaw-root-of-trust-csmesecurity-vulnerability. Accessed 24 Sept 2020
36. WhatsApp LLC (2020) How to back up to iCloud. WhatsApp Web. https://faq.whatsapp.com/iphone/chats/how-to-back-up-to-icloud/. Accessed 28 Sept 2020