Strong cryptography in the 21th century: the key to democracy

Wietze Beukema, student Computer Science

April 2015

Introduction

As of 2015, encryption can be found anywhere. Compared to the previous decade, it has become increasingly easy to obtain software with strong encryption. For instance, messaging service WhatsApp provides end-to-end encryption on devices to protect its users from potential eavesdropping. Not to mention the majority of the larger Web companies that enforce traffic to their website over a secured connection (BuiltWith, 2015).

However, there is still an ongoing debate on the issue of strong encryption in a modern democracy. Although there are various advantages of having encryption available to the people, encryption also brings some downsides that might have a profound impact on democracy and society. As the discussion is still going on, there is so far no consensus on what place strong encryption should have in a democracy.

The primary objective of this paper is to examine how strong encryption might interfere with or strengthen democracy, and how encryption should be used in a democracy in order to protect both democracy and liberty. First, a brief history of electronic encryption is discussed. Secondly, the impact of strong encryption on democracy is analysed. In the third part, it is investigated why it is hard to establish a compromise in which both proponents and opponents of strong encryption are partly satisfied. Finally, a conclusion on the main question of this essay is given and discussed.

In answering these questions, this essay focusses on democracy. However, as we will see, the democratic elements in the context of strong encryption are closely related to liberty. After all, one might define democracy a set of concepts and ideas about freedom.

Historical context

Various kinds of encryption have been used throughout history; the desire to communicate without being eavesdropped is of all ages. Before the 21th century, encryption has been a cumbersome, time-consuming activity. After machines became common, scientists realised how machines could significantly speed-up encryption and make it easier in use.

The first time it became visible how valuable encryption can be, was during the Second World War. Nazi Germany used the Enigma cipher to encrypt its military communication (Kahn, 1996). Although the data transmitted by the Germans could be received by anyone with an antenna, due to the encryption the Enigma added, the information that was transmitted looked like gibberish to outsiders. Only receivers who had access to an Enigma machine and were in possession of the right key could decrypt the data and obtain the original text. After the British were able to crack the cipher, the Allies had a great source of information to anticipate on; it is

estimated that thanks to breaking the cipher, the war was shortened by a few years (Singh, 1999, pp. 186-187).

In the years following the Second World War, the Cold War era, Western countries realised how powerful encryption was for military purposes. As a result, the use of encryption was strongly regulated in those countries. The United States introduced export restrictions on technologies such as encryption in order to prevent it falling into the hands of the Eastern bloc. At this time, it was illegal to distribute programs of machines that contained encryption to areas outside the United States or countries of its allies (Singh, 1999).

Until the Cold War, encryption was mainly used for military purposes. This changed when shortly after the Cold War the first encryption suites became available to the wide public. Well-known is Phil Zimmermann's *Pretty Good Privacy*, better known as PGP, which was introduced in 1991. PGP is a free tool that provides tools to safely store files and exchange messages. As Zimmermann made the program freely available on the Internet, the tool became rapidly popular amongst users around the world. As this included countries outside the West, the FBI started a formal investigation against Zimmermann. As encryption was, due to its use for military purposes, included in the US Government's definition of munitions, Zimmermann was allegedly illegally exporting a 'weapon' (Singh, 1999, p. 303). After several years, the investigation was closed without filing charges against anyone.

An interesting case regarding government involvement in encryption is the Clipper Chip (Denning, 1994). In 1993, the United States government introduced the communication chip, which was available to US vendors to implement in their products. The chip could, for instance, be implemented in a landline phone in order to provide a secure line; both sides of a phone call would need a device that has the Clipper Chip on board. What made the Clipper Chip unique, was that the United States government had access to the keys that were used to encrypt the communication. Using a key-escrow scheme, in which two independent government bodies possessed both 50% of the key, the government could look-up decryption keys and obtain the original data transmitted (Denning, 1994).

By this means, according to the US, the people could secure their communications against eavesdroppers while the government still had a way to get in if necessary. For example, if criminals would use Clipper Chip products, the investigation bureau would tap their phone lines, decipher the communication and hence still be able to hear what they are discussing over the phone, just like police forces were able to do before encryption was widely available. In other words, the goal of the United States government for this initiative was to build its surveillance interests into the products of the increasingly privacy-aware citizens. The Clipper Chip was not successful; in 1998, the Clinton Administration concluded that the opposition to key escrow was too great (Pednekar-Magal & Schields, 2003).

Most countries, in particular Western countries, have taken measures against terrorism in reaction to the attack on the World Trade Centre took place in 2001. After these terrorist attacks, many nations have introduced new legislation in order to secure the national security such as smart passports, intelligence sharing between nations and intensified (data) surveillance. As encryption, now freely available to everyone, might hinder police forces and intelligence services in their work, the discussion about encryption intensified.

Impact on democracy

It can be concluded from the brief history of strong encryption that governments have a mixed relationship with it. On the one hand, they use it themselves to secure their own communication, while on the other hand, they want to restrict its use for individuals and companies for (national) security reasons.

Before we discuss arguments to allow or restrict the use of strong cryptography, we should consider why this technology raises new issues that we cannot solve with established norms. Still today, cryptography is characterised as a weapon: it can play an important role in military operations, it can be used in good and bad ways, and hence it is argued that it should be regulated as a 'dual-use good' (Shehadeh, 1999). But is it realistic to consider encryption similar to a weapon? Let us take a closer look at the PGP case. PGP was criticised by government officials as they argued that by exporting crypto, one is basically exporting a weapon. The community of PGP users disagreed and tried to find ways to make sure that PGP could be distributed without restrictions. In 1995, Zimmerman published a book that contained the complete source code of the PGP software. By publishing the source code in book form, it was protected under the First Amendment (freedom of speech and freedom of press) and could be legally shipped abroad. Here, it is obvious that the notion of a 'weapon' becomes ambiguous when it involves cyberspace. The weapon here is a piece of software, which can be expressed in programming (source) code, which is information, and the expression of that information is a protected right. 'Exporting' it is also a vague term in this context as it concerns distribution over the Internet. It is hardly comparable to the export of tangible goods, which are physically transported and go through customs. Also, the fact that there can be made unlimited copies (as it involves digital information) makes it very different from traditional weapons. Hence, encryption is although somewhat comparable to, definitely not the same as a traditional weapon. Therefore, we cannot apply the same norms and rules we have for traditional weapons, but we should rather come up with new, specific norms and rules for this situation.

As a consequence, encryption raises a technical question that has political consequences. Encryption in itself is just a product of mathematics and programming code; however, how it is used and (possibly) regulated impacts democracy and society. Ever since electronic encryption became widely available (through the Internet) governments have struggled regulating it. Encryption can support democracy in several ways, while it may also affect democratic principles.

Privacy

There are multiple arguments that support the use of strong encryption in a democracy. The most straightforward argument is that encryption can support the right to privacy. Although there is not a single, all-embracing definition for privacy, it is often defined as the right to be in control over your own personal information (Introna, 1997).

Privacy can protect individuals against external threats. Moor (1997) for instance claimed that privacy in itself is not a core value, but it is the expression of the core value of security. Without security, cultures don't survive and flourish. He considers privacy a "critical, interlocking member of our systems of values in our increasingly computerized culture". It has been argued that privacy is not merely concerned with the individual, but that it is a value of contributing

the broader social good and that within this line of reasoning it follows that privacy is essential for maintaining democracy (Westin, 1967).

It has also been argued that privacy should be preserved to support individual development (Introna, 1997). Without privacy, there would be no 'self'. Knowing to being watched changes one's behaviour, which makes it a lot harder to create an authentic identity. With privacy, any individual can decide on his own whether or not to abide the moral code of society. Following this reasoning, it is hard to create a genuine opinion on a political matter without privacy. Related to this, as we will see later on, is the freedom of expression.

Especially the computerisation makes the urge for privacy bigger. Because the computer is a 'logically malleable tool', as Moor has put it, it is easier to infringing one's privacy. Due to their unprecedented computing capacity, computers raise serious privacy concerns. Consider the following example: in earlier ages, the primary means of long-distance communication used to be mail. In order for someone to eavesdrop on this means of communication, one had to physically obtain the letter. In order to avoid suspicion of tampering, the eavesdropper would have to steam it open and return it to its original condition afterwards. This required a lot of time and precision, which does not scale up. In comparison, in the digital age, it is significantly easier to obtain such information: most communication channels pass a single entry point that can be eavesdropped. Using smart algorithms, interesting information can be subtracted from all the information that passes by, without the sender or receiver noticing that they are being eavesdropped.

Freedom of expression

Related to the previous one, the second argument is that strong encryption helps supporting the freedom of expression. Freedom of expression is generally thought to be a fundamental prerequisite for a genuine democracy. Freedom of expression can be generally defined as the ability to one's right to communicate one's opinions and ideas.

In Mill's view, freedom of expression is a very important liberty. In *On Liberty*, he notes that there ought to exist the liberty of discussing anything; any doctrine, no matter how immoral it may seem to anyone else. Silencing one's opinion is "robbing the human race": if the opinion is right (supposing an opinion can be right or wrong) mankind is deprived of the opportunity to hear that opinion. Even in the case were an opinion is 'wrong', the people are deprived from the clearer perception of truth, a result of its collision with error (Mill, 1869). In other words, freedom of expression helps us to push arguments to their limits and get the best discussion possible.

With regards to a democracy itself, freedom of expression is a requirement to secure the political rights of individuals. It gives each individual the opportunity to support political thoughts or ideologies without having to fear what expressing this view might implicate. Equally, individuals can protest or express non-compliance without worrying how their position might affect their role in society. Hence, it is fundamental to the democratic process.

Strong encryption can support freedom of expression. Consider a person who lives in a society where there exists no encryption. If this person wants to express his views on a certain topic, he might feel restricted to do so, as everything he says is public to everyone and can be traced back to him. The person might feel embarrassed about a certain opinion or might be afraid that

certain people will disapprove of him for his views. In the extreme case, he might even get harmed by other people for having this opinion. Encryption can, in adherence with Mill's Harm Principle, prevent that from happening by securing one's information in such a way that it is only readable to those who that person chooses to.
In particular, strong encryption is used by political activists to communicate from authoritarian regimes with the outside world without the government being able to eavesdrop. In conclusion, strong encryption is also in this respect fundamental to the democratic process.

Freedom of expression is, however, not limitless or absolute: there are multiple ways in which this freedom collides with other values. According to Mill's Harm Principle, freedom of expression can be overruled in order to prevent harm to others (Mill, 1869). Common nowadays examples of limits on freedom of expression include hate speech, defamation, disclosing classified information and violation of copyright.

(National) security

Ever since encryption has become commonplace, there has been one major counterargument regarding the use of strong encryption. As criminals move with the times, their activities move into cyberspace (Nissenbaum, 2005). Opponents have often argued that strong encryption makes it harder for police forces and intelligence agencies to do their work, as they are unable to read encrypted communication or encrypted stored data.

As these institutions were in the past able to wiretap phones of criminals, the increased use of secured communication channels can make it virtually impossible to apply the same methods as a few decades ago. Thus, the wide deployment of strong encryption might make fighting crime harder, compared to the pre-encryption era. This might conflict with the concept of retributive justice. Also, it might be harder to prevent crime; this conflicts with Mill's Harm Principle.

As we have already seen, privacy and freedom of speech are important values in democracy, although they are not absolute rights in this context. In the discussion on privacy, there is a general consensus that privacy might in some cases be overridden, for instance when national security is at stake. This principle is often applied in the offline world, e.g. by search and seizure laws. Enforcing this same principle in cyberspace raises problems. Consider what would happen if strong encryption was applied to every digital communication channel and every storage medium. It would be virtually impossible to override privacy concerns for more important matters. Hence, strong encryption almost *makes* privacy an absolute right, as there is by default no way to circumvent it, even when there are valid reasons to infringe on one's privacy.

The question now arises whether this right to privacy is in fact more important than any other aspect of democracy. Especially after the terrorist attacks on the World Trade Centre on September 11, 2009, the debate around civil rights and national security interests has become more intense. If we again evaluate this balance using Mill's Harm Principle, one might argue that state intervention is an effort to prevent harm to other people by the state. In this sense, limiting privacy can be justified if it prevents harm. The ongoing debate however remains to what extent privacy can be infringed on to achieve what level of prevention of harm. Note that it is often unclear how many harm is prevented by breaching one's privacy and makes it as a consequence difficult to discuss if it was justified.

Suggested solutions

Obviously, there is a conflict between privacy and security when it comes to the use of strong encryption. We have seen that one the one hand, strong encryption is an irreplaceable tool we have for maintaining democracy; on the other hand, it might conflict with freedoms, resulting in serious harm. Complete prohibition of strong encryption is not desirable at all, as we have argued that strong encryption protects core values of democracy.

It does not immediately follows that therefore strong encryption should be fully allowed. Instead, another solution has been proposed: allowing encryption, but only encryption schemes that are designed in a way that governments can obtain the original unencrypted data when this would be justifiable without having the original key. This compromise would, according to the proponents, solve the problem, as it would allow individuals and organisations to safely communicate and store sensitive information without intervention of unauthorised people, while authorities can in justified cases still obtain the necessary data. As FBI General Counsel Valery Caproni stated in 2010: "[Software vendors] can provide strong encryption. They just need to figure out how they can provide us plain text".

In a way, this concept might sound promising, as it tries to preserve privacy as much as possible while maintaining the possibility of authority intervention if necessary. While it remains debatable when it is justifiable to break one's privacy, it is worthwhile to investigate what such a system ought to look like.

Weaken encryption

The first time in which a government regulated the use of encryption in order to maintain security interests, was in the 1990s. At that time, governments such as the United States government restricted the maximum length of encryption that was allowed; the maximum encryption strength was bounded by the strength at which the intelligence services were still able to crack the encryption (Singh, 1999).

However, this approach is untenable. Even though encryption can still be applied, due to the weak encryption, this gives a false sense of security. The major objection is that not only governments will be able to crack the cipher, but also outsiders. And if not only governments but also outsiders can obtain access to the original data, all reasons to have encryption in the first place are basically thrown away.

Also, this concept implies that an intelligence service could decrypt all encrypted data they gathered, which opens the door to abuse. If government agencies can decrypt all information they intercept, there is no one to check whether they only do this in justified cases. Even if breaking encryption has to be approved by court, there is no way to be certain the intelligence services abuse their power. This approach is thus vulnerable to fraud and abuse by both governments itself and others.

Trusted third party

A second approach is government involvement in the encryption schemes in use, generally called *trusted third party* solutions. A strong encryption scheme is used in which a third party, in this case a government institute, holds 'spare keys' that can be used to decrypt encrypted information without having the original keys. A major advantages of this over the previously discussed approach is that this system can be made compatible with the system of checks and

balances, by requiring a court order before handing over the spare keys. This is the same concept the Clipper chip was based on.

Despite the failure of the Clipper chip, many governments remain convinced that key escrow can be made to work. Most recently, the British Prime Minister Cameron stated that he intends to 'stop the use of methods of communication that cannot be read by the security services' (Griffin, 2015) by forcing big tech companies to build-in backdoors. The US government and the EU counter-terrorism coordinator supported this view (Burton, 2015). Hence, the idea of government involvement in encryption remains alive.

Despite the fact that the approach might look promising, it suffers from some serious practical problems. First of all, the very fact that an encryption scheme has a built-in backdoor means that the scheme is flawed by design. Even if somehow it could be guaranteed that a government will only use the backdoor in very serious situations, there is no guarantee that hackers will be able to use the same backdoor to obtain information. The fact that an extra attack vector is added to an encryption scheme which again, as with the previous approach, will give outsiders an opportunity to obtain access to the original information, gives a false sense of security.

In addition, since there is already a vast amount of non-key escrowed systems available, it is not very likely that criminals would switch to government-controlled encryption; basically, it is already too late for that. Since criminals are likely to avoid government-controlled systems, this solution would overshoot the mark. The only way to have a chance to make this effective would be the prohibition of other schemes; this however obviously conflicts with democratic principles of freedom.

Finally, other practical issues such as how to organise a key escrow infrastructure and how to guarantee that the escrowed keys are solely used for genuine purposes remain uncertain. In summary, this approach might seem appealing but is in practice not feasible.

Mandatory key disclosure

Finally, a somewhat related approach involve the mandatory disclosure of encryption keys by individuals or companies. The United Kingdom has since 2007 a law in force which requires suspects to supply decryption keys to government representatives with a court order. In case a suspect refuses to do so could result in a penalty up to two years in jail.

Also this approach has some serious issues. A main concern is that there is no way to be certain that one knows or knows how to obtain the key. People do in fact forget about keys; therefore, one could go to jail for forgetting a password. In case people stored the key in some safe place, the key could have got lost. The only way to prevent this from happening, is being certain that someone knows the key or how to obtain it but refuses to disclose it; however, being certain about this is obviously impossible.

A more fundamental issue this approach violates right against self-incrimination and the right to silence, which are broadly accepted rights in democracies. So again, this approach infringes on fundamental liberties ought to be present in democracy. Therefore, this concept is in many perspectives undesired.

Discussion

Democracy relies on a number of core values, including open debate, freedom of opinion and political participation. In an era where technology plays such a dominant role in most people's life as a means of communication, it is essential that democratic values are also protected in technology. The most efficient way to mitigate the threats that technology impose on democratic values, such as hacking and data surveillance, is by using strong encryption. Strong encryption is therefore a crucial safeguard of democracy in the 21th century.

As we have seen in the previous section, the suggested compromises provide no real solution to the problem; they all either give a false sense of security or seriously conflict with other principles. It is therefore argued that the only feasible solution is to fully allow strong encryption.

Although this might imply that the work of police forces will become more complicated, it is certainly not the only way to convict criminals or prevent crime. Besides the lack of evidence that supports the claim that without encryption we would have less harm, it should also be noted that there are numerous alternatives to make strong cases and being effective in preventing harm without having the ability to eavesdrop on communication or having access to encrypted files. Restricting the use of encryption is too rigorous considering the resulting side effects on democracy.

The future of the status of strong encryption remains unclear, as it is likely that governments will continue to struggle with this problem. Especially the tendency to fear heavily influences the debate on this issue, as opponents emphasise how strong encryption might support organised crime and terrorists in their activities. In a time where the news is dominated by stories of war and terrorism, it is appealing to go along with these sentiments. Hopefully, this essay contributes to a more rational debate on this important issue.

Bibliography

BuiltWith. (2015). *SSL by Default Usage Statistics*. Retrieved March 15, 2015, from BuiltWith: http://trends.builtwith.com/ssl/SSL-by-Default

Burton, G. (2015, January 23). *EU swings behind David Cameron's encryption plan.* Retrieved March 15, 2015, from Computing: http://www.computing.co.uk/ctg/news/2391793/eu-swings-behind-david-camerons-encryption-plan-as-party-grassroots-voice-opposition

Denning, D. (1994). The US key escrow encryption technology. *Computer Communications, 17*(7), 453-457.

Griffin, A. (2015, January 12). *WhatsApp and iMessage could be banned under new surveillance plans.* Retrieved March 15, 2015, from The Independent: http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-and-snapchat-could-be-banned-under-new-surveillance-plans-9973035.html

Introna, L. D. (1997). Privacy and the Computer: Why We Need Privacy In the Information Society. *Metaphilosophy, 28*(3), 259-275.

Kahn, D. (1996). *The Code Breakers.* New York: Scribner.

Mill, J. (1869). *On Liberty.* London: Longman, Roberts & Green.

Moor, J. H. (1997). Towards a Theory of Privacy in the Information Age. *Computers and Society, 27*(3), 27-32.

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology, 7*, 61-73.

Pednekar-Magal, V., & Schields, P. (2003). The State and Telecom Surveillance Policy: The Clipper Chip Initative. *Communication Law and Policy, 8*(4), 429-464.

Shehadeh, K. (1999). The Wassenaar Arrangement and Encryption Exports: An Ineffective Export Control Regime that Compromises United States Economic Interests. *American Univ. Int'l L. Rev.*, 283-84.

Singh, S. (1999). *The Code Book.* New York: Anchor Books.

Westin, A. F. (1967). *Privacy and Freedom* (Vol. 59). New York: Atheneum.