European Journal for Security Research (2022) 7:39–65
https://doi.org/10.1007/s41125-022-00080-0

ORIGINAL ARTICLE

U.S. Security Policy: The Dual-Use Regulation of Cryptography and its Effects on Surveillance

Thea Riebe[1] · Philipp Kühn[1] · Philipp Imperatori[1] · Christian Reuter[1]

Received: 18 October 2021 / Accepted: 17 January 2022 / Published online: 26 February 2022

Abstract
Cryptography has become ubiquitous in communication technology and is considered a necessary part of information security. However, both the regulation to restrict access to cryptography, as well as practices to weaken or break encryption, are part of the States' security policies. The United States (U.S.) regulate cryptography for export in international trade as a dual-use good. However, the regulation has been increasingly loosened and transferred to bilateral agreements with Information and Communication Technology companies. At the same time, the National Security Agency attempted to implement a government encryption standard to guarantee itself easier access to data, thus progressively expanding surveillance on non-U.S. citizens. In this paper, using comparative policy analysis, we examine the evolution of both security policies by tracing the historical development of U.S. regulation of cryptography as a dual-use good, and surveillance technologies, and practices used from the 1990s to today. We conclude that the impact of the dual-use regulation has affected the efficiency of surveillance technology, by loosening regulations only for mass communication services, thereby supporting the proliferation of surveillance intermediaries, while working on strategies to collaborate and exploit their coverage.

Keywords Cryptography · Surveillance · NSA · Dual-use regulation

1 Introduction

Today, numerous cryptographic algorithms ensure the availability, confidentiality, and integrity of our data. They are ubiquitous in today's information and communication technology (ICT) devices and services, most of the time being used in the background, such as the TLS protocol (Krawczyk et al. 2013), which is used to provide confidential web browsing. Cryptography is one of the central aspects of

✉ Thea Riebe
riebe@peasec.tu-darmstadt.de

[1] Science and Technology for Peace and Security (PEASEC), Technical University Darmstadt, Darmstadt, Germany

information security, as it prevents unauthorized access to information, thus maintaining and ensuring the information's confidentiality and integrity (Abutaha et al. 2011). The strength of a cryptographic algorithm is measured by its used security key's length.[1] This is based on the fact, that cryptographic algorithms are secure by design, i.e., the only weak link is the cryptographic key, which needs to be brute forced, to maliciously access the encrypted information.[2] While this might offer great security at one point of time, it might be weakened by advances in computing capacity which makes breaking encryption faster.[3] The access to cryptographic algorithms exceeding a certain key length (in the following paper bundled under the term cryptography) has been regulated and restricted, while intelligence and law enforcement agencies have worked to break or circumvent encryption to access data.

The trade of cryptography is regulated internationally as a dual-use good and is subject to export and import restrictions (Vella 2017; Wassenaar Arrangement Secretariat 2017). As cryptography has become omnipresent in communication technology, it is to currently regulated as a dual-use good like nuclear technology components, biotechnological instruments, and certain chemical tools. However, unlike the aforementioned dual-use goods, cryptographic innovations and products are not likely to be part of a weapon system or an improvised weapon (Forge 2010). Nor does it seem to be dual-use in the sense that the technology can be used in beneficial and harmful ways (Evans 2014, p. 277). Then, why is cryptography considered dual use? The answer lies in the security policies which assess the risks of unsecured IT against the risk of "going dark" (Comey 2014). Restricting access to cryptographic innovation seems to be guaranteeing access to encrypted information and the possibility of "global commercial and state-led mass surveillance" (Monsees 2020).

Since the United States (U.S.) industry was a global leader in developing computers and communication technologies early on (Southard 1997) and currently dominates the application-based IT market with companies like Apple, Alphabet, and Amazon (Andriole 2018), it has access to diverse information about customers all around the world worthy of protection (Giles 2018). Likewise, U.S.-based companies have significant dominance in the global cyber security software market: in 2015, their market share was near 61% (Australian Cyber Security Growth Network 2018). However, this economic strength is accompanied by a restrictive security policy. Cryptographic tools were even regulated as a weapon in the U.S. for

[1] Since symmetric cryptographic algorithms usually offer the same security strength as their key length, the strength of other cryptographic families (like asymmetric encryption using elliptic curve cryptography) is given as their symmetric counterparts, e.g., the strength of 3072-bit RSA or a 256-bit elliptic curve are both equivalent to its 128-bit symmetric counterpart in terms of security. Current cryptographic systems consider a symmetric key-strength of 128bit and more to be secure (Barker and Roginsky 2019).

[2] This assumption has been shown to be false for some encryption algorithms and has always been tested by security experts searching for security flaws in an algorithms' design. But there are, of course, other ways to access encrypted information, e.g., by blackmailing, threatening, or compromising a computer system.

[3] One example is the DES algorithm with 40bit key length, which offered a reasonable security in 1975, but was easily crackable in 1998. Another aspect is technological advancement like quantum computers, which might make a whole family of cryptographic algorithms insecure (Electronic Frontier Foundation 1998).

several decades until 1994 and were prohibited to be exported due to strong regulations (Black 2002). The National Security Agency's (NSA) global surveillance and espionage programs, revealed by the publication of classified documents by former NSA agent Edward Snowden beginning in 2013, cast an unprecedented perspective on U.S. security policy. Moreover, it was mostly U.S. products with worldwide distribution that were infiltrated in these programs (Daniel Castro 2020). In the following years, new immense and expensive surveillance programs were built to overcome encryption on a global scale. At least to date, both, export regulations and the work of the NSA, remain essential instruments of U.S. policy on encryption. However, it is unclear in what way and to what extent cryptography is restricted, and how this continues to influence recent calls for the complete ban of "warrant-proof" encryption (ibid.). Subsequently, to analyze the regulation of cryptography as a dual-use good and the practices of the national security organizations in the U.S. from the 1990s to today, we ask: *Why was the regulation of cryptography liberalized for mass communication services from 2000, while the surveillance politics focused on similar services?*

To compare the historical policy development, and the dual-use regulation, and surveillance policy, this paper first illustrates the related work (Sect. 2). In the following, the method of research, data collection, and policy analysis are described (Sect. 3). The results (Sect. 4) compare the dual-use and surveillance policies during three time periods in the 1990s (4.1), the 2000s (4.2) and the 2010s (4.3), providing the historical and technological context of the periods. This is followed by a discussion of the results (Sect. 5) and a conclusion (Sect. 6).

2 Related Work

The security policies regarding cryptography are part of many scientific discourses and disciplines. The discourse on surveillance and securitization of cryptography are discussed in Sect. 2.1, while the related work concerning the regulation of cryptography as a dual-use good is discussed in Sect. 2.2., followed by the research gap in Sect. 2.3.

2.1 Surveillance Studies Perspective on Security Practices

The increased access to information technology for private users as well as for security organizations has led to the increased use of "surveillance-oriented security technologies" (SOSTs). SOSTs are technologies that are designed to monitor terrorists and criminal groups but are also capable of and have been used to monitor the public on a large scale (Degli Esposti & Santiago Gómez 2015, p. 437; Pauli et al. 2016). The acquisition of SOSTs has been legitimized as means to prevent criminal and terrorist attacks; however, it has also led to critical discussions of surveillance measures (Ball et al. 2012; Bauman et al. 2014; Bigo 2006; Lyon 2006). Kaufmann (2016) illustrates how the technologization of security lead to "the rhizomatic" spread of surveillance, not only top down, but fragmented and without a single sovereign power, as described by Haggerty and Ericson (2000) as an assemblage. Kaufmann (2016, p. 93) argues that this assemblage is distinctive of the security governance, as it "occurs in parallel, sometimes in complementary and sometimes in conflicting forms: security practices are undertaken in the mode of military and disciplinary access, in the mode of legally oriented police work, and in the mode of preventing and preempting political risks."

The contradictions of security governance have also been discussed by Poscher (2016) who argues that in criminal law there is a "heightened sense of vulnerability" which drives the changes of law towards, among others, the internationalization of security threats (which we can also observe regarding the use of cryptography), the blending of prevention and repression, as well as the blending of police and secret services. The governance of the secret services seems to pose some challenges, as their programs and practices are usually not debated within the public sphere. This leads to "a conundrum", as the same organizations which are obliged to protect the democracies are undermining them at the same time due to the lack of transparency (ibid., p. 69). The public discourse on the capabilities of secret services is also discussed by Murphy (2020), who stresses the need for a democratic debate that moves away from the scandal-driven narrative of a binary choice between user privacy and "unfettered state access to communication". In his analysis, Murphy (2020) compares four types of legal instruments to gain access to communication by the Five Eyes states (USA, UK, Australia, Canada, and New Zealand). He concludes that a broad range of legal means have already been implemented, yet they lack public awareness and oversight, because efforts to and questions on how to apply such legislation are met with questions over jurisdiction, as the internet cannot be confined to the borders of any nation state, due to its "cross-territorial nature" (ibid., p. 258).

Security policies aim to govern encryption, because it is driving up the cost of surveillance. Clayford and Piesters (2018) have analyzed the effectiveness of surveillance technology, as it is legitimized and perceived by U.S. and U.K. intelligence officials through their public statements. They found that effectiveness feeds into what is seen as proportionate, as well as on the legal framework regarding privacy and the overall costs of the operations. In addition to the evolution of the use of cryptography, Kessler and Phillips (2020) trace the debate regarding legal issues, particularly in relation to privacy. Like Murphy (2020), they conclude that the installation of backdoors or vulnerabilities is not desirable due to the security ramifications.

In contrast to the U.S, the EU Commission opposed key escrow plans already in 1997 ("EU Commission Rejects U.S. Plan on Encryption 1997"). In 2016, the European Union Agency for Cybersecurity (ENISA) repeated this statement and justified its stance by stating that backdoors are not effective in combating criminal activity and instead undermine the security of the digital society. The negative effects of such an approach could thus in turn be observed in the U.S. Instead, ENISA advocates strong encryption as a safeguard for the individual's right to privacy (ENISA 2016).

2.2 Governance of Cryptography as a Security Relevant Dual-use Good

To control goods that can be used as parts of weapon systems or for military applications, trade regulations serve as a tool for security policy to control the proliferation of technologies. Internationally, the Wassenaar Arrangement is a multilateral export control regime, which has 42-member states. These states agree on lists and definitions for relevant technologies, which are regularly updated. However, the arrangement is legally non-binding (Wassenaar Arrangement Secretariat 2021). Therefore, especially in the case of cryptography, as well as regarding the origin of many ICT services and companies, regulation adopted by the U.S. is internationally relevant to users and customers of ICT products. The current trade regulation of cryptography is presented and summarized based on U.S. laws in the comparative study by Vella (2017). She describes in detail the legal categorization of cryptography assets and the distribution of enforcement roles among authorities, and briefly considers the historical development of the legislation internationally. She concludes that in contrast to the EU, the U.S. has aligned their concept of dual-use with national security interests legitimized by the war on terror, while the EU has integrated human security as an important argument to support the proliferation of encryption technologies. Like the U.S., the EU follows a broad definition of the scope of encryption controls and incorporates activation codes. However, the EU has always included “mass-market” components. Moreover, unlike the U.S., the EU clearly defines what falls under control and what does not. However, there is no uniformity of export regulations among EU member states. While countries are united in their dedication to liberal encryption regulation and export control laws are subject to European law, the implementation of these laws can be subject to the interpretation of member states. In some cases, they may interpret the regulation differently or have additional national laws. Furthermore, military goods, for example, are regulated solely by national export regulations (ibid.).

Similarly, Saper (2013) compares the regulation of encryption technology internationally and outlines the export policy and its implications and provides practical recommendations for exporters on how to manage them. While applying strict restrictions on the export of cryptography, the U.S. does not, however, restrict the use or import of cryptography. When exporting cryptography, which is not designed to be part of medical end-use, or to protect intellectual property functions, the primary factor is the key length. Encryption products that provide keys above a certain threshold face export restrictions (ibid., p. 680). However, “mass-market products”, like e-mail encryption products, are excluded. Nevertheless, the domestic use of cryptography has been scrutinized as well. Landau (2015) points out, how the NSA influenced the recommended encryption standard by the National Institute of Standards and Technology (NIST) which was not considered secure and would have allowed easy decryption by outsiders. In her article, she draws various parallels between the NSA’s past and current actions, specifically referring to the controversy surrounding a possible backdoor of the 1970s Data Encryption Standard (DES) with the attempts regarding the standard Dual Elliptic Curve Deterministic Random Bit Generator (Dual EC_DRBG). Schulze (2017) makes a similar comparison between the Clipper Chip program and the Snowden revelations, while he restricts the study to NSA activities and mostly excludes the regulating policy. He highlights the similarities in the arguments of officials who claim that encryption impedes effective law enforcement, seeking to establish "the norm of government control over cryptography vs. the right of every user to communicate privately" (Schulze 2017). The increasing use of encryption is more so a reaction to the previous, inconsiderate, and in part unlawful actions of states. Van Hoboken and Rubinstein (2014) focus on the organizational and technical responses to the disclosure of transnational surveillance by the NSA in a historical context. Using the cloud service industry as an example, they show that providers mostly responded by implementing even stronger privacy protections and advanced cryptographic protocols, which in turn raises the question of how the U.S. government may deal with this increased resistance to surveillance. Deconstructing the security discourse, Monsees (2019, p. 81) shows how encryption has been turned into a question of security policy, as not only a matter of "the state" vs. "the public", but rather "various forms of publicness emerge, or their emergence is complicated by the prevailing security narratives".

These narratives have been evolving ever since. After Edward Snowden revealed the programs and extent to which the NSA deployed surveillance technologies until 2013, the U.S. introduced two new laws, the EARN IT Act and the Lawful Access to Encrypted Data Act (LEADA) in 2020, which regulate the access of security agencies to user data (Figas 2020; Pfefferkorn 2020). While the EARN IT Act enforces the implementation of commissions within tech companies to formulate best practices dealing with content on social media platforms for example, LEADA has been criticized to force companies to provide backdoors for law enforcement agencies while making end-to-end encryption unlawful. This shows how the laws regarding encryption, legal decryption, as well as import and export restrictions for dual-use goods, influence the access to cryptography for U.S. and non-U.S. citizens.

2.3 Research Gap

Considering the recent approaches to prevent potential criminals from "going dark" (Pfefferkorn 2020), it seems contradictory that the regulation of cryptographic technologies for mass communication technologies has been liberalized since the year 2000, even before most of the mass communication and social media companies had been founded and become internationally successful. And although the key length remains one of the most important characteristics to measure the security of encryption, concerning regulation, however, key length has become less important. As the literature on SOSTs and cryptography politics has acknowledged the effects of dual-use regulation on the effectiveness of surveillance technology use, the historical development of both policies and its interactive effects have not been compared in detail. Further, the role of intermediaries as proliferators of encryption and surveillance infrastructure has gained little attention (Kaufmann 2016; Rozenshtein 2018). Therefore, this paper contributes to this discourse by comparing the security policies regarding dual-use regulation and surveillance programs.

Table 1 Overview: Regulative foundations

Type	Dual-use goods	Military goods
Law on control	Export administration act (EAA)	Arms export control act (ACEA)
Authorized authority	U.S. Commerce Department's Bureau of Export administration (BXA)	U.S. Department of State
Definition of regulations	Export administration regulations (EAR)	International traffic in arms regulations (ITAR)
Control list	Commerce control list (CCL)	U.S. Munitions List (USML)
Maximum waiting time for a decision on exports	120 days (Dam and Lin 1996)	Unlimited (Dam and Lin 1996)

3 Method

The paper aims to examine encryption policy measures in terms of evaluating encryption as a dual-use technology. Therefore, a comparative literature analysis will be conducted, considering regulative foundations, scientific publications as well as journalistic works. In the following, we will describe the specifics of our research method.

3.1 Data Collection

For the data collection, primarily the databases Google Scholar and Springer Link were used to select scientific publications that focus on regulations. For ease of comparison, current regulations and historical intelligence activities are additionally examined so that a comparative analysis is possible. Table 1 shows the regulative foundations for dual-use goods. The summary of the NSA's activities is based on the paper "The U.S. Surveillance Programs and Their Impact on EU Citizens' Fundamental Rights" published by the European Parliament (Bowden 2013). The revelations and programs of the NSA are summarized in Table 2. For analyzing the NSA programs solely journalistic works using at least three of the four keywords "Snowden", "Encryption", "BULLRUN" and "NSA" are considered.

3.2 Data Analysis

Based on the selected documents, our analysis aims to highlight regulatory attempts of the U.S. cooperation with the NSA. Therefore, we use policy analysis in general and the approach of policy process. To do so, we selected a small number of cases where cryptography has been used to outline different cryptography practices conducted by (1) the U.S. government, and (2) by the NSA. Tables 1 and 2 provide an overview of the two further types of selected documents: (1) regulatory foundations for the practices of the U.S. government, and (2) the different

Table 2 Overview of NSA programs

NSA Program	Specialization
PRISM	Surveillance program with access to servers operated by large (groups of) companies (Google, Microsoft, Apple, Yahoo, YouTube, Facebook, AOL, and Paltalk) (Greenwald et al. 2013a, b,)
Upstream collection	Data collected by intercepting transoceanic cables and surveillance of communication data of numerous providers (Timberg 2013; Timberg and Nakashima 2013)
XKeyscore	Far-reaching surveillance program that was used to monitor the individual internet activity (visited websites, chats, emails, transmitted documents, metadata) of people all over the world in real time. Because of the amount of data, it was only stored for a limited number of days (Greenwald 2013b)
BULLRUN	Decryption program in which various encryption technologies were compromised, loopholes were installed into existing systems, and global cryptography standards were manipulated (J. Ball et al. 2013)

NSA programs following up on the U.S. regulatory attempts. Generally, the policy process approach focuses on political processes and the involved stakeholders, while the scope lies on the broader meso-scale. In this context, this aims at determining what processes, means, and policy instruments, e.g., regulation, legislation, or subsidy, are used. Within this policy process, the role and influence of stakeholders needs to be discussed (Hult 2015). In our analysis, the relevant stakeholders identified include those already mentioned (the U.S. Government and NSA), as well as the (4) civil society and (5) economy. Against the background of our selected policy field, these stakeholders have been chosen based on an examination of the dual-use export politics and their related practices, as well as the security agency's policies.

Following the typology of (Gerring and Cojocaru 2016), we conduct a two-case causal analysis and compare our selected cases longitudinally in three different time periods. Since we want to identify the causes of our outcomes, namely the *surveillance policies* and *dual-use policies,* the case study can be described as exploratory: The outcome (Y) is specified and framed as a research question—in our study, "Why does Y occur?". Thus, the purpose of our study is to identify X, which is considered a possible cause of Y (Gerring and Cojocaru, 2016). To compare the two outcomes, it is necessary to develop comparison categories. As described, means and policy instruments as well as relevant stakeholders are the focal point of our analysis. Furthermore, the public perception and the usage of cryptography seem to be relevant factors for policy implementation. Based on these considerations, we identified several guiding questions to develop our comparison categories. Accordingly, the categories derived for the comparison are (1) *targeted actors, (2) implementing organizations, (3) methods and regulations, and context factors such as (4) developments in cryptography and usage* (see Tables 4, 5).

We conduct a longitudinal case study by referring to three different time periods (see Fig. 3). We chose these periods as they are all characterized by specific events and attitudes and are thus distinct from each other. The first period is defined by key escrow as the main strategy of the U.S. government, expressed in the attempted implementation of the Clipper Chip (T1: 1990–2001, see Sect. 4.1).

However, with September 11 and the resulting Patriot Act, a new period of U.S. surveillance policy began in 2001, characterized by mass surveillance by the NSA. At the same time, major tech companies, such as Twitter and Facebook, emerged (T2: 2001–2013, see Sect. 4.2). This period ends with the revelations of Edward Snowden, during which the BULLRUN program became public. Our third chosen period can therefore be considered the post-Edward Snowden era (T3: 2013–2021, see Sect. 4.3). End-to-end encryption is increasingly becoming the standard, and users' content is no longer accessed by companies as intermediaries between private industry and politics. In this context, the "going dark" debate is gaining momentum, and research into exploits is increasingly coming into focus.

4 Results

4.1 The 1990s: Cryptography and the Internet Become Accessible

The 1990s were marked by significant innovative breakthroughs in technological development—not least manifested in the development and commercialization of the World Wide Web (WWW). As the internet emerged as a network of networks, which were connected to exchange information and businesses, the question of encryption also became a discourse that would significantly shape the next years of technological development. Due to the commercialization of the internet, cryptography became more important for the needs of companies and end-users, which challenged the monopoly of the government over the technology (Sircar 2017, p. 29f.). The historic development is outlined in Table 6 (see Appendix) showing how the level of security and the categorization of cryptography changed. While in 1992 nine types of encryption were excluded from regulations[4] (Grimmett 2001, pp. 5–6), and only a few goods with a weak 56-bit symmetrical encryption were tolerated, key escrow was becoming the method of choice since it met both the interest of economy and prosecution (Dean 1999, p. 11).

To bring the industrial and government sectors under one umbrella, as early as April 16, 1993, the White House planned a voluntary program to improve communications security and privacy, considering prosecution authorities' requirements (The White House 1993). First, this was put into practice using a hardware module called Clipper Chip (The White House 1993), based on NSA competencies (Anderson 1996, p. 79). It was developed to decrypt conversations and was built into appropriate devices such as telephones (Dam and Lin 1996). A symmetrical encryption algorithm called "Skipjack" with an 80-bit key length incorporating a key escrow technology that was developed by the NSA (Hodkowski 1997) is illustrated in Fig. 1.

[4] These 9 types of encryption include: (1) decryption of copy-protected software; (2) use in machines for banking or money transactions; (3) cryptographic processing using analog functions in certain broadcast and fax equipment; (4) personalized smart cards; (5) access control, such as in ATMs; (6) data authentication; (7) fixed data compression or coding techniques; (8) reception of limited- audience radio or television programs (decryption must be limited to video, audio or management functions; and (9) anti-virus software (Grimmett 2001).

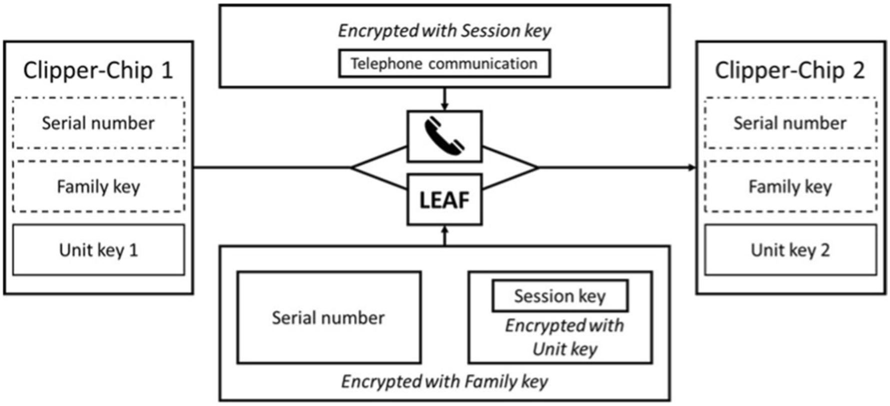
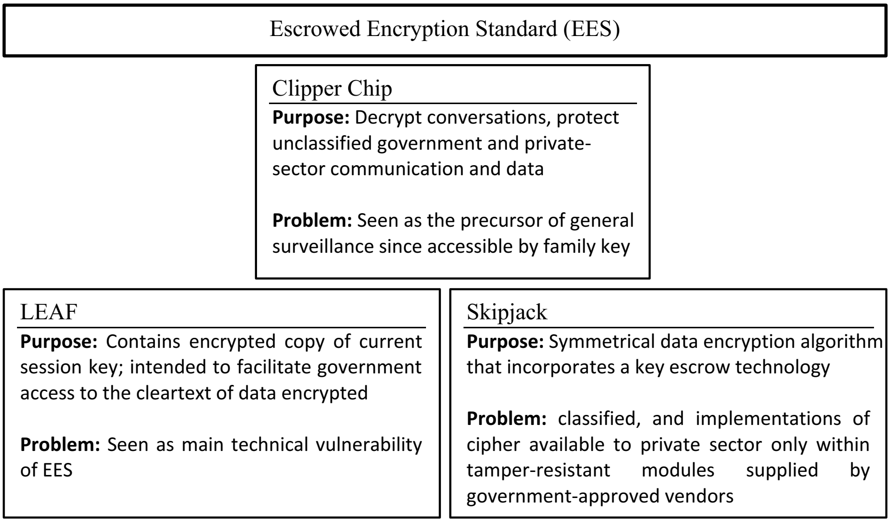


Fig. 1 Representation of the communication of two clipper chips (own illustration)



Escrowed Encryption Standard (EES)

Clipper Chip

Purpose: Decrypt conversations, protect unclassified government and private-sector communication and data

Problem: Seen as the precursor of general surveillance since accessible by family key

LEAF

Purpose: Contains encrypted copy of current session key; intended to facilitate government access to the cleartext of data encrypted

Problem: Seen as main technical vulnerability of EES

Skipjack

Purpose: Symmetrical data encryption algorithm that incorporates a key escrow technology

Problem: classified, and implementations of cipher available to private sector only within tamper-resistant modules supplied by government-approved vendors

Fig. 2 Outline of the main encryption practice before 2013 (own illustration). The shown encryption standards and methods have been developed by the NSA to ensure access to information

While the used symmetric encryption was 2^{24} times more secure, it was backdoored using the key escrow functionalities, enabling law enforcement agencies to decrypt the Law Enforcement Access Field (LEAF) which was part of each transmission and hence knew the involved chips' serial numbers. However, authorities needed court orders to request device keys matching the serial numbers. This allowed them to get the session keys that were included in the LEAF and to decrypt communications (Dam and Lin 1996).

Ten months later, this method became Federal Information Processing Standard (FIPS) under the name “Escrowed Encryption Standard” (EES, see Fig. 2, Black 2002; U.S. Department of Commerce and National Institute of Standards and Technology, 1994). However, only a few goods including the Clipper Chip, (approximately 10,000–15,000) were sold or installed, while most of them were bought by the U.S. administrative itself to convince manufacturers launching these programs (Banisar and Davies 1998; Schulze 2017). Until the Clipper Chip had become an established, inevitable standard, concerns arose over its voluntary nature and it potentially remaining transient (Shearer and Gutmann 1996, p. 130). The main objection to the Clipper Chip was the proposed key collection system that was seen as a precursor to general surveillance. Anyone who wanted real security would either use other programs or use the Clipper Chip to add a second layer of non-government-approved encryption (Shearer and Gutmann 1996, p. 130). At the end of 1995, the Clipper Chip initiative was considered to have failed, despite all governmental efforts. As the NSA had withheld information on the detailed technical background of the algorithm when it was introduced, this calls to question the agency's trustworthiness, as security should always rely on the secret key but not security-by-obscurity (Dean 1999).

There were two main developments in 1996: On the one hand, President Clinton transitioned encryption software from USML to the CCL and altered regulation from the Department of State to the Department of Commerce through Executive Order 13,026. In general, the Clinton Administration enacted new measures to reform the encryption export regulations by permitting more powerful encryption technology and enabling mass-marketing of higher strength encryption products (Eichler 2018, p. 13). On the other hand, since 1996, cryptography has been assessed as a dual-use technology, should the security level limit, the maximum non-regulated symmetrical key length, be exceeded. However, with the exponential increase in computing powers and thus increasing abilities of stronger attacks on encryption (Moore 1965), cryptography needed to keep up with this progress, for which key length negatively correlates with the likelihood of decryption. Figure 3 shows the requirements for the key length (in bits) of cryptographic procedures because of technological developments, as well as the respective legally allowed key length. A distinction is made between short-term and long-term security of 20 years. The axiom of the recommended key length is that cryptography is secure if decryption would take an intelligence service with $300 million funding several months. These assessments trace back to the report of Blaze et al. (1996a, b). Furthermore, since 1998, the NSA has been using malware to tap data before computers encrypt it (Gallagher and Greenwald 2014), while not detectable and remotely controllable (Boon et al. 2013). Further, it was planned to automatize these efforts on a large scale to infiltrate millions of computers (Gallagher and Greenwald 2014). In terms of dual-use, a liberalization of U.S. export policies started in 1998, when the Clinton administration announced a new policy to reform the previously strict export regime.

Generally, it can be observed that due to increased digitalization, cryptography became important for companies and for civilian purposes. Especially for global actors, the problem of the necessity to export encryption arose, which was prohibited by U.S. regulations. However, not least due to the increasing societal relevance and commercialization of the internet, there is a growing public discourse on the role of encryption that went beyond a solely organizational debate. While in the

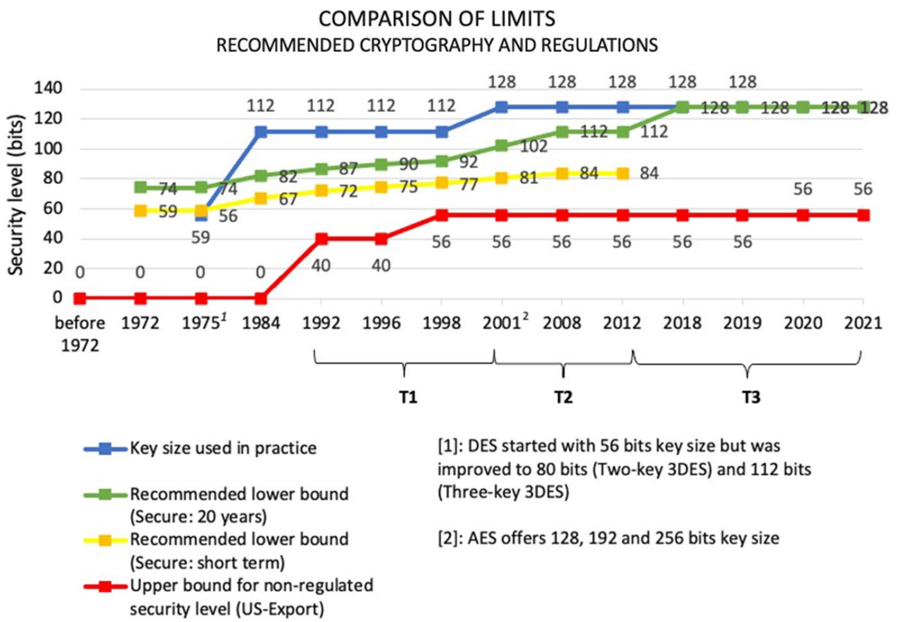


Fig. 3 Recommended security levels compared with their regulations (own illustration, data source: Abdalla et al. 2018; Babbages et al. 2009; Blaze and Diie et al. 1996a, b.; ENISA 2014)

1990s communication encryption was used only by a few, there were critical voices from the security community demanding stronger encryption policies (Sircar 2017).

4.2 The 2000s: The War on Terror and the Spread of Social Media

The historic context changed with the attacks on the World Trade Center on 9/11, which led to the War on Terror and to legislation increasing the abilities of law enforcement agencies, such as the Patriot Act. On the technological side, from the early 2000s on, social media companies emerged and expanded their user group from the U.S. to Europe and across the world. Along with the emergence of social media, publicly available data and communication increased, leading to research on big data for surveillance purposes. These globally active companies not only sold their customers' data for profit but also became relevant as surveillance intermediaries for law enforcement agencies (Rozenshtein 2018). Due to their access to millions of consumers' data and the lack of regulation, concerns on privacy arrived and led to the first users of open-source end-to-end encryption software, OpenPGP (OpenPGP: About 2020).

In the year 2000, key length was no longer the only important factor for export licenses, as exporting mass-market cryptography of all key lengths became possible. March 2010 marks a significant change in export regulations, with, U.S. President Barack Obama's announcement to reform of the export controls of cryptography to facilitate trade and innovations (Fergusson and Kerr 2018). Prior to this reform,

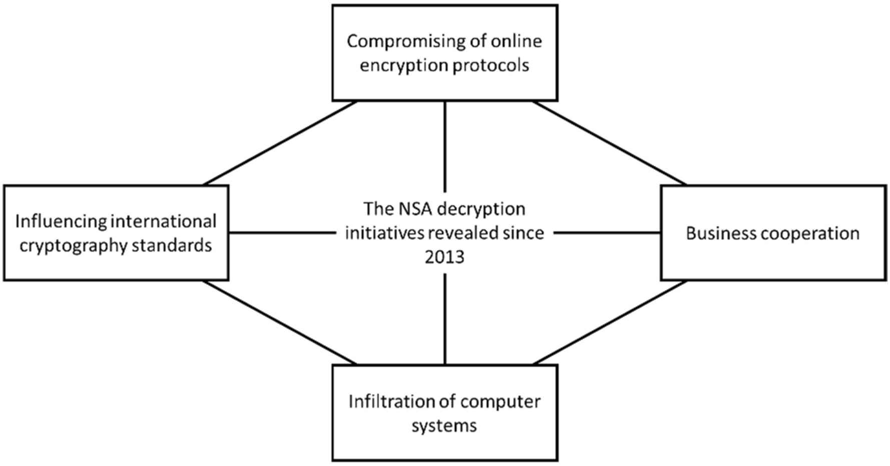

Compromising of online encryption protocols
Influencing international cryptography standards
The NSA decryption initiatives revealed since 2013
Business cooperation
Infiltration of computer systems

Fig. 4 The NSA's decryption initiatives (own illustration)

most exporting manufacturers had to pass a 30-day long technical examination (Fergusson and Kerr 2018). After the reform, exporters only needed to register the exports to the Commerce Department and the NSA by mailing and sending a report of export sales to the Commerce Department at the end of the year (U.S. Department of Commerce 2010).

In 2013, secret programs by the NSA were revealed by NSA agent Edward Snowden. The information shed public attention on espionage activities of the NSA and were essential for the further evaluation of U.S. cryptography policy, stimulated a societal debate on *privacy* and data *security,* and brought the debate on cryptography policy into focus. In this context, the Guardian exposed an NSA program confirming their practices of continuously registering the metadata of millions of phone calls in the network of a large telecom operator (Greenwald 2013a). Especially the confidential NSA program BULLRUN was focused on the work with cryptography to be able to survey communication in the future (Cayford et al. 2014, p. 646). This was achieved by influencing international cryptography standards, using immense computing capacities of supercomputers, as well as by cooperating with technology companies and internet providers (Ball et al. 2013). A leaked guide for NSA employees revealed that the program was used to survey VPN, VoIP, and SSL (Ball et al. 2013). Apart from that, the NSA was able to decrypt the stream cipher A5/1 (Timberg and Soltani 2013), allowing it to easily access billions of phone calls and SMS messages (ibid.). In its SIGINT Enabling Project, the NSA worked with technology companies and an annual budget of 250 million dollars aiming to pursue manufacturers to purposely add weaknesses to commercial encryption systems (ibid.). The computer and network security company RSA was given 10 million dollars by the NSA for including a backdoor as key escrow to their encryption software (Menn 2013). A comparison between the EES program and BULLRUN can be found in Table 3.

Table 3 The NSA's decryption programs

Category	Development of EES	Project "BULLRUN "
Time of start and disclosure	1993 and 1993	2000 and 2013
Surveyed data	Phone and data communication in the USA	Phone and data communication worldwide
Concept	Development of a state-run encryption method with a backdoor	Breaking and manipulating existing encryption methods
Restrictions to guarantee privacy	The key was only delivered by the two U.S. authorities when a court order existed	No restrictions
Main beneficiary	Prosecution	National security
Transparency	Public announcement of the implementation but non-disclosure of the used method	Non-disclosure of the project as a whole
Success	Execution failed	Effective for decrypting communication surveyed by other NSA projects

In some cases, the NSA pressured companies into providing keys or installing backdoors by taking legal action against them (Larson 2013). Some stated that numerous keys were in the hands of the NSA because of its efforts to hack corporate networks (Perlroth et al. 2013). The NSA kept an internal database of keys for specific commercial goods (ibid.). An internal report explicitly explains how the NSA has regularly received routers, servers, and other computer network devices of U.S. manufacturers, functioning as an intermediate stop on the distribution journey, installing a backdoor technology for surveillance and then repacking the goods with a factory seal and exporting them (Greenwald 2014). Moreover, the NSA built a backdoor into the algorithm Dual EC_DRBG which NIST treated as encryption standard, later followed by the "International Organization for Standardization" and its 163 member states (Landau 2015; Perlroth et al. 2013). Additionally, the NSA worked on a quantum computer to break virtually all types of asymmetric encryption (Rich and Gellmann 2014).

Worldwide, the NSA infected 50,000 computer networks with malware to access sensitive information and to control various functionalities (Boon et al. 2013), including microphones, webcams, and histories together with login details (Gallagher and Greenwald 2014). These attacks were executed by a special department called Office of Tailored Access Operations (TAO), now Computer Network Operations, which consisted of more than a thousand hackers (Boon et al. 2013; Gallagher and Greenwald, 2014). Following a Washington Post report which appeared in 2013, all 16 U.S. intelligence agencies had an annual budget of 50 billion dollars (Gellman and Miller 2013). The following Fig. 4 shows the crosshairs made of the NSA's fundamental methods to avoid cryptography.

Summarized, the exposure of NSA surveillance programs contrasts with the historically lengthy process toward liberalized cryptographic regulation. The outlined practices show, (1) how the U.S. government's attempts at regulation in cooperation with the NSA have not led to sufficient results and (2) how intelligence agencies have sought unofficial avenues. In the years between 2001 and 2013, the increasing use of end-to-end encryption in commercial communication goods led to a liberalization of the export of dual-use goods. Nevertheless, there were still restrictions of certain stronger encryption products, especially outside of mass communication goods, e.g., for cryptography within military goods (Eichler, 2018). However, after the end of the Clipper Chip initiative, the strategy of law enforcement agencies started to shift towards the use of vulnerabilities and the cooperation with ICT companies as surveillance intermediaries (Greenwald et al., 2013a, b). The same companies, however, profited from the liberalization of dual-use export regulations.

4.3 The 2010s: From the Snowden Revelations to Today

Due to the increasing computing power, new challenges for encryption technologies arise today. The excessive use of internet-enabled devices such as smartphones also formulates new requirements on encryption. This is a time when big data analytics has become mainstream (Stieglitz et al. 2018). As previously elaborated, adopted U.S. regulations have consistently fallen short of recommendations for short- and long-term security, and the U.S. government's policy assessment of cryptography based on key length can be judged restrictive rather than liberal. This discrepancy is illustrated by the fact that any encryption using the minimum required key length would be classified as a dual-use item, and that the limit on items that may be exported and not classified as dual-use items was last raised in 1998 to 56-bit. This value is maintained, even though NIST recommends the use of keys with a minimum strength of 112-bits of security to protect data until 2030, and 128-bits of security thereafter (ENISA, 2013)—more than double the value and consequently implying a 2(128–56) = 272 times larger range of keys. Thus, it can be argued that the "too slow" and too restrictive regulation of cryptography on the part of the U.S. government has not been able to keep up with the rapid pace of technical progress, leaving room for unofficial ways of intelligence agencies.

Notably, there was not only a lack of anticipation of technical development, but also a lack of public discourse. Only after project BULLRUN produced an international backlash and increased the urge to use end-to-end encryption in messenger services such as Facebook and WhatsApp (Isaac 2019), has a more active social discourse emerged – not only in the U.S., but worldwide, which is why Monsees speaks of a social sensibilization (Monsees 2020). The intelligence and law enforcement officials have since taken the public perception of surveillance technology into account (Cayford and Pieters 2018).

This led to the discussion of two new bills, making access to user data legally available by the support of the ICT companies. In March 2020, the U.S. Congress proposed the EARN IT Act, aiming to combat child abuse material online (Figas 2020). This is based on Sect. 230, which states that online platforms cannot be held liable for the content of users on their platforms. According to the EARN IT Act, providers need to earn this immunity by complying with a set of guidelines developed by a commission of experts within the company (Pfefferkorn 2020). These guidelines will probably affect end-to-end encryption (Pfefferkorn 2020) since law enforcement officials have the option to search the data stored on servers to find criminal material online. By weakening end-to-end encryption, the data of all internet users will be less secure (Jordan and Polk 2020). The second initiative is the Lawful Access to Encrypted Data Act of 2020, a bill to ban providers from offering any encryption that cannot be decrypted or by law enforcement (Pfefferkorn 2020). This bill covers providers who recorded one million or more users annually in any year since 2016, if data is stored. When the data is in motion like in communication, providers with more than a million monthly active users in any month since January 2016 are affected by the ban. To access encrypted material, law enforcement needs a warrant based on a probable cause (LeClair 2020). With law enforcement able to decrypt data stored on servers, companies cannot offer end-to-end encryption to their users anymore. Either they have the option to build backdoors into their encryption or not to use encryption at all (Olmstead and Polk 2020). The massive roll-out of end-to-end encryption after Edward Snowden's revelation of the BULLRUN program primarily increased the costs for the NSA to collect and decrypt communication. Both legal initiatives are still in discussion, however, they show how security agencies face increasing financial and legal pressure (Savage 2020).

The export of cryptography with a key length of 128 bits or more is considered as dual-use, which simplifies the export of strong encryption methods such as AES.

Generally, most of the omnipresent cryptography technologies are currently still classified as dual-use and regulated by the Commerce Control List (Maurer et al. 2014; Schwechter 2016). Goods with strong encryption require an export license unless they are distributed to Canada (Schwechter 2016). Contrary to this, weak cryptography is not subject to strict regulations; as a license, it is only required for trades to terror-supporting or embargoed states (ibid.). Presently, the CCL controls goods exceeding the 56-bits threshold for symmetrical cryptography and the 512-bits threshold for asymmetrical cryptography (Vella 2017). In today's age, encryption with this key length is considered weak (Saper 2013). However, as the U.S. Commerce Department Bureau of Industry and Security (BIS) elaborated: a broad range of license exceptions differentiating between various types of products, end-users, core benefits, and export destinations are included in the law (U.S. Department of Commerce 2020). Moreover, for defense companies, the rules have been relaxed (Eichler 2018, p. 27f.), so that sensitive electronic data is not considered to be classified as an "export good" if the data is end-to-end encrypted. There would be only a few forms of cryptography, including stronger ones, that could not be exported because of these license expectations (ibid.). For example, cryptography positioned as a mass-market good only requires an inquiry for categorization or a self-disclosure to the U.S. Commerce Department when it is at 64-bits for symmetrical encryption and 768-bits for asymmetrical encryption (U.S. Department of Commerce 2016, p. 2). Furthermore, open-source cryptography is not affected by the export controls if the BIS is informed via email (U.S. Department of Commerce 2020). This also simplifies the export of strong encryption methods such as AES. Only certain goods are still controlled: those of military nature, quantum key distribution, or cryptography for ultra-wideband systems (ibid.).

5 Discussion

To answer the research question: *Why was the regulation of cryptography liberalized for mass communication services from 2000, while the surveillance politics focused on similar services?,* we compared the historical development of surveillance and dual-use policies in the U.S. in three time periods (1990–2021). Analyzing the development of dual-use regulations and the surveillance policies, we found it puzzling how mass communication services have been excluded from 2000 on. In the 1990s, the *dual-use regulations* were adapted to the increasing access to cryptography as part of the commercial internet (see Table 4). This was acknowledged, by changing the legislation from the United States Munition List (USML) to the Commerce Control List (CCL), while also enforcing the implementation of key escrow for symmetrical encryption. However, with the rising use of encryption, the exceptions and key lengths accelerated until 2000. In the 2000s, the use of end-to-end encryption increased, which made the key escrow approach impractical. The products for mass-marked communication have been excluded from the dual-use export restrictions, which were still in place for other exports with market encryption at up to 64-bits following a technical examination. However, the bureaucracy was further removed, requiring only self-reports and many exceptions, or even supporting the use of end-to-end encryption for military goods

Table 4 Summary of the relevant surveillance practices outlined in the results

Dual-use Regulation	1990s	2010s	2020s
Targeted Actors	(1) Exporting companies (2) Non-U.S. citizens	(1) Exporting companies (with exceptions regarding the sector and key length) (2) Non-U.S. citizens (until 2010)	(1) Exporting companies (with exceptions regarding the sector and key length)
Implementing Organizations	•USML→ CCL	•CCL •BXA → BIS, Department of Commerce	•CCL •BIS, Department of Commerce
Measures and Regulations	•Prohibition •Classification as weapon/dual-use item •Liberalization since 1998 for mass communication products	•Unilateral controls •Export license for goods with strong encryption •Trade-deregulation since 2010	•Dual-use: key length of 128-bits or more •Simplification of strong encryption exports •liberalization to support encryption of military information and goods (2016)
Changes in Cryptography	•Symmetric keys •Problematic export	•Public-key-encryption (end-to-end) became more used	•E2EE •Distributed reimplementation of social media platforms

Table 5 Summary of relevant surveillance practices outlined in the results

Surveillance Practices	1990s	2010s	2020s
Targeted Actors	(1) Manufacturing companies	(1) Companies as intermediaries (2) U.S. and non-U.S. citizens	(1) Companies as intermediaries (2) U.S. and non-U.S. citizens
Implementing Organizations	•Law enforcement agencies, •Secret Services	•Law enforcement agencies, •Secret Services	•Law enforcement agencies, •Secret Services
Measures, Programs and Regulations	•Key Escrow •Clipper Chip •Skipjack •LEAF	•BULLRUN •SIGINT Enabling Project	•EARN IT •LEADA
Innovations in Cryptography	•Proven insecurity of old standards	•Facilitation of trade/innovations •Reduced bureaucracy •Bypass/break of encryption exports	•Formation of privacy-focused tech-companies •Surveillance as a service (NSO)

and information since 2016 (Eichler 2018). Today, the export of cryptography with key length of 128 bits or more is considered dual-use. Within the U.S., the import, or domestic sales of cryptography, however, were never restricted.

The *surveillance policy* in the 1990s (see Table 5), in alignment with the dual-use policy, was developed to ensure a key escrow mechanism with the Clipper Chip initiative. In the 2000s, mass communication services became popular, as well as the first possibilities to implement end-to-end encryption for end-users. To retrieve data, security agencies made a bilateral agreement between the ICT companies and exploited weak encryption standards or software vulnerabilities. This way, intelligence organizations, like the NSA, profited from the export restrictions in two ways: First, the increased and global use of social media platforms and other commercial services for mass communication which did not use strong encryption. And second, as these companies would provide data to law enforcement agencies.

Edward Snowdon's revelations have drawn public awareness to the debate on cryptography. Consequently, U.S. companies had to rebuild their reputation and image: Apple and Alphabet reacted by establishing automatic encryption that makes it near to impossible to provide data even after a court order (Timberg 2014). They also cooperate in a coalition called Reform Government Surveillance with companies such as Amazon, Dropbox, and Microsoft (Reform Government Surveillance (RSG) 2020). They publicly stand up for privacy and the limitation of surveillance. Numerous companies expanded their security measures with investments running into the millions and started a digital arms race against the NSA (Perlroth and Goel 2013). The U.S. has developed legal instruments that improve the possibility to access data by enforcing the cooperation of ICT companies (Murphy 2020). As a result, ICT companies have faced pressure from both sides: from the government to implement different forms of key escrow, as well as from the customers, and have become surveillance intermediaries (Rozenshtein 2018). Murphy (2020, p. 260) states that the "increase in use of encryption is an example of escalation—a response to reckless (and unlawful) behavior by states in the past" and describes the "back door" as dual-use, as it is not only for the "good guys". However, surveillance technologies proliferate in a fragmented way driven by a diversity of factors and different sectors (Haggerty and Ericson 2000; Kaufmann 2016). The proliferation is influenced by the costs for decryption and effectiveness of surveillance as well as the public discourse. These factors influence what is perceived as proportionate (Cayford and Pieters 2018) to legitimize the use or surveillance technologies.

Looking at current innovations in cryptography, such as better performance in asymmetric encryption technologies with Elliptic Curve Crypto (ECC) or the research in the field of quantum computing, key length, with respect to the symmetric counterparts (see Sect. 1), will still be an important measurement to determine, whether a cipher can be considered secure. Moreover, it enables researchers to discuss the strength of cryptographic algorithms (Paterson 2015). Innovations in cryptography usually impact the computational capabilities of machines, which required longer key lengths or a new family of cryptographic algorithms. Such impacts are currently discussed with the development of quantum computers, which, if they become available, can solve currently known mathematical problems. This would break currently popular asymmetric cryptographic algorithms and thus, require new standards. Moreover, quantum computers also impact symmetric cryptographic algorithms due to their properties, which would require twice the key length for the same security (Bennett et al. 1997). Besides the key length, other factors also impact the security of cryptographic algorithms (Paterson 2015). One such factor is the actual implementation of the cryptographic algorithm. It might be implemented with vulnerabilities compromising the otherwise mathematically proven to be a secure algorithm. Another factor is the system itself, which is used for cryptographic operations since it might be compromised. These organizational factors of security; however, can be created or unknowingly taken advantage of by companies which are forced to implement access to their data by the government to prevent users to "go dark" (Murphy 2020). Many states, e.g., in the EU have evoked ideas of legal state hacking; however, without paying enough attention to the safeguards towards these methods (Koops and Kosta 2018). In addition, there is a growing industry which offers "surveillance as a service", in which law enforcement agencies and secret services outsource the technological hacking capacities or to exploit software vulnerabilities when needed, instead of building the capacity themselves (Kirchgaessner et al. 2021). This makes the use of the service more flexible for organizations. However, the proliferation and use of such services is difficult to safeguard, as the U.S. has put the NSO Group on a trade blacklist, because it has conducted "transnational repression [..] targeting dissidents, journalists, and activists" (Clayton 2021).

Our research has *limitations:* First, the information that we have about current surveillance programs is very limited. To our knowledge, there is no information if and how the surveillance programs by the NSA are continued. Only little is known from fact-finding committees, like in Germany, which only focused on the cooperation between the BND and the NSA (Gopalakrishnan 2016). The surveillance by the NSA of non-U.S. and non-EU citizens needs to be further studied, focusing on the quality and quantity of surveillance technologies, as well as the question of global coverage while there is a lack of political representation in the discourse on proportionality. Regarding the assessment of metadata surveillance, a comparison to the discourse on data preservation programs by internet providers can be drawn (Riebe et al. 2020). Second, the ambivalent role of ICT companies as surveillance intermediaries needs further investigation. In addition, the case of the surveillance software Pegasus has shown how intelligence organizations partly outsource surveillance technologies (Kirchgaessner et al. 2021). This reduces the already difficult process of attributing accountability for surveillance practices.

6 Conclusion

Encryption of information is ubiquitous and serves to secure most of today's ICT infrastructure. This paper has illustrated how the regulation of cryptography as a dual-use good as well as the practices of the US intelligence and law enforcement agencies to break or weaken encryption have developed since the 1990s. While the regulation of dual-use goods has been liberalized, ICT companies have become both allies of and antagonists to the secret services. Strategies to break encryption or work around encryption using key escrow approaches, like the Clipper Chip, have been unsuccessful, due to public backlash and security vulnerabilities of the system and thus moved to bilateral agreements and cooperation with individual companies. Further approaches to regulate and break encryption, as well as public discourse to outlaw strong encryption, have shown how the security narratives are still used up to this day. As the restrictions of the export of cryptography have been liberalized to some extent, they help to reinforce the surveillance through the exceptions for surveillance intermediaries. The authors conclude that as surveillance technologies are increasingly proliferating, the role of ICT as surveillance intermediaries needs to be further discussed. Recent attempts to ban law enforcement-proof encryption should be used to foster a discourse on the transparent process of balancing the conflicting security interests and the means of intelligence and law enforcement organizations.

Appendix

Acknowledgements This work was supported by the German Federal Ministry for Education and Research (BMBF) in the project CYWARN (13N15407), KontiKat (13N14351) and VIOLENCE (01UG2203E). Further, we would like to thank the anonymous reviewers for their thoughtful comments as well as Hannah Appich and Lilian Reichert for their assistance in preparing the manuscript.

Funding Open Access funding enabled and organized by Projekt DEAL. Technische Universität Darmstadt,FIF IANUS Interdisciplinary Research Funding,German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts, National Research Center for Applied Cybersecurity ATHENE

Table 6 Historical development of the regulations of cryptography in the U.S

Year	Level of security and categorization of cryptography	Most important legislative changes
Before 1992	More than 0-bit, weapon	•All exports required a license
1992	More than 40-bit, weapon (partly dual-use)	•9 types of encryption were seen as a dual-use technology
1996	More than 40-bit, dual-use	•An exception of the export ban was possible after a technical assessment when goods were focused on the mass-market •Exports of symmetrical encryption at up to 56-bits: required a plan on how key escrow would be implemented •Exports of encryption of all security levels: required a backdoor for prosecution matters •Waiting time was reduced to 40 days
1998	More than 56-bit, dual-use	•Exports of encryption with a more flexible key length to banks, financial institutions, or actors in the medical field
2000	More than 56-bit, dual-use	•Key length was no longer important for export licenses •Exporting mass-market cryptography of all key lengths was possible •Possible license exception for mass-market encryption at up to 64-bits following a technical examination
2010	More than 56-bit, dual-use	•Reduced bureaucracy for certain exports: technical assessment for less sensitive or most mass-market encryption was no longer required •Instead, a registration and a self-report were required
2019	More than 56-bit, dual-use	•Many different types of license exceptions for all kinds of encryption, provided some criteria are met
Currently (2021)	128-bit, dual-use	•The access to user data is made legally available by the support of the ICT companies

References

Abdalla M, Bellare M, Neven G (2018) Robust encryption. J Cryptol 31(2):307–350. https://doi.org/10.1007/s00145-017-9258-8

Abutaha M, Farajallah M, Tahboub R, Odeh M (2011) Survey paper: cryptography is the science of information security. Int J Comput Sci Secur (IJCSS) 5(3):298–309

Anderson RJ (1996) Crypto in Europe—markets, law and policy. In: Dawson E, Golić J (eds) Cryptography: policy and algorithms. Springer, Berlin. https://doi.org/10.1007/BFb0032347

Andriole S (2018) Apple, Google, Microsoft, Amazon And Facebook Own Huge Market Shares = Technology Oligarchy. *Forbes Magazine*. https://www.forbes.com/sites/steveandriole/2018/09/26/apple-google-microsoft-amazon-and-facebook-own-huge-market-shares-technology-oligarchy/?sh=347277342318

Australian Cyber Security Growth Network (2018) Global cyber security software market share by company domicile. In Australia's cyber security: sector competitiveness plan. https://www.austcyber.com/tools-andresources/sector-competitiveness-plan-2018

Babbages S, Catalano D, Cid C, de Weger B, Dunkelmann O, Gehrmann C, Luis G, Lange T, Lenstra A, Mitchell C, Näslund M, Nguyen P, Parr C, Paterson K, Pelzl J, Pornin T, Preneel B, Rechberger C, Rijmen V, Ward M (2009) ECRYPT2 yearly report on algorithms and Keysizes. https://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.7.pdf

Ball K, Haggerty KD, Lyon D (eds) (2012) Routledge handbook of surveillance studies. Routledge, London

Ball J, Boger J, Greewald G (2013) Revealed: how US and UK spy agencies defeat internet privacy and security. The Guardian. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Banisar D, Davies S (1998) The code war. Index Censorship 27(1):162–168. https://doi.org/10.1080/03064229808536306

Barker E, Roginsky A (2019) Transitioning the use of cryptographic algorithms and key lengths. Doi: https://doi.org/10.6028/NIST.SP.800-131Ar2

Bauman Z, Bigo D, Esteves P, Guild E, Jabri V, Lyon D, Walker RBJ (2014) After snowden: rethinking the impact of surveillance. Int Polit Soc 8(2):121–144. https://doi.org/10.1111/ips.12048

Bennett CH, Bernstein E, Brassard G, Vazirani U (1997) Strengths and weaknesses of quantum computing. SIAM J Comput 26(5):1510–1523. https://doi.org/10.1137/S0097539796300933

Bigo D (2006) Security, exception, ban and surveillance. In: Lyon D (ed) Theorizing surveillance: the panopticon and beyond. Routledge, pp 46–68

Black SK (2002) Encryption. In: Adams R (ed) Telecommunications law in the internet age. Morgan Kaufmann Publishers, Burlington, pp 327–387

Blaze M, Diffie W, Rivest R, Schneier B (1996a) Minimal key lengths for symmetric ciphers to provide adequate commercial security January

Blaze M, Diie W, Rivest RL, Schneier B, Shimomura T, Thompson E, Wiener M (1996b) Falls church VA 22042 performing organization number(s) sponsoring/monitoring agency name(s) and address(es) defense technical information center DTIC-IA 8725. In John J Kingman Rd. https://apps.dtic.mil/sti/pdfs/ADA389646.pdf

Boon F, Derix S, Modderkolk H (2013) NSA infected 50,000 computer networks with malicious software. Nrc.Nl. https://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software-a1429487

Bowden C (2013) The US surveillance programmes and their impact on EU citizens' fundamental rights. In: Policy department C: citizens' rights and constitutional affairs

Daniel Castro (2020) Why new calls to subvert commercial encryption are unjustified. ITIF. https://itif.org/publications/2020/07/13/why-new-calls-subvert-commercial-encryption-are-unjustified

Cayford M, Pieters W (2018) The effectiveness of surveillance technology: what intelligence officials are saying. Inf Soc 34(2):88–103. https://doi.org/10.1080/01972243.2017.1414721

Cayford M, van Gulijk C, van Gelder P (2014) All swept up: An initial classification of NSA surveillance technology. In: Nowakowski T, Młyńczak M, Jodejko-Pietruczuk A, Werbińska-Wojciechowska S (eds) Safety and reliability: methodology and applications. CRC Press, Boca Raton

Clayton J (2021) Apple sues Israeli spyware firm NSO group. BBC News. https://www.bbc.com/news/business-59393823

Comey JB (2014) going dark: are technology, privacy, and public safety on a collision course? FBI. https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

EU Commission Rejects U.S. Plan on Encryption (1997) The Wall Street Journal. https://www.wsj.com/articles/SB876322992856833000

Dam KW, Lin HS (1996) Cryptography's role in securing the information society. National Academies Press, Washington, DC

Dean P (1999) A right to private digital communication? Updating the debate. Converg Int J Res New Media Technol 5(3):8–14

Degli Esposti S, Santiago Gómez E (2015) Acceptable surveillance-orientated security technologies: Insights from the surprise project. Surveill Soc 13(3–4):437–454. https://doi.org/10.24908/ss.v13i3/4.5400

Eichler RR (2018) Cybersecurity, encryption, and defense industry compliance with united states export regulations. Texas a&m J Prop Law 5(1):8–9

Electronic Frontier Foundation (1998) Cracking DES: secrets of encryption research, wiretap politics, and chip design. O'Reilly. https://web.archive.org/web/20080731155316/http:/cryptome.org/cracking-des/cracking-des.htm

ENISA (2013) Algorithms, key sizes and parameters report—2013. https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report

ENISA (2014) Algorithms, key size and parameters: report. ENISA. https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

ENISA (2016) ENISA's opinion paper on encryption strong encryption safeguards our digital identity. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption

Evans NG (2014) Dual-use decision making: relational and positional issues. Monash Bioeth Rev 32(3–4):268–283. https://doi.org/10.1007/s40592-015-0026-y

Fergusson IF, Kerr PK (2018) The U.S. Export control system and the export control reform initiative (Version 44). https://sgp.fas.org/crs/natsec/R41916.pdf

Figas L (2020) USA: Der EARN IT Act—analyse und Kritik. Boxcryptor. https://www.boxcryptor.com/de/blog/post/earn-it-act-a-threat-to-end-to-end-encryption/

Forge J (2010) A note on the definition of "dual use." Sci Eng Ethics 16(1):111–118. https://doi.org/10.1007/s11948-009-9159-9

Gallagher R, Greenwald G (2014) How the NSA plans to infect 'Millions' of computers with malware. The intercept. https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

Gellman B, Miller G (2013) 'Black budget' summary details U.S. spy network's successes, failures and objectives. The Washington post. https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

Gerring J, Cojocaru L (2016) Selecting cases for intensive analysis. Sociol Methods Res 45(3):392–423. https://doi.org/10.1177/0049124116631692

Giles M (2018) It's time to rein in the data barons. MIT technology review. https://www.technologyreview.com/2018/06/19/240453/its-time-to-rein-in-the-data-barons/

Gopalakrishnan M (2016) German court's ruling on mass spying is a victory for the BND and NSA. Deutsche Welle. https://www.dw.com/en/german-courts-ruling-on-mass-spying-is-a-victory-for-the-bnd-and-nsa/a-36402749

Greenwald G, MacAskill E, Poitras L, Ackermann S, Rushe D (2013) Microsoft handed the NSA access to encrypted messages. https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

Greenwald G (2013a) NSA collecting phone records of millions of Verizon customers daily this article is more than 8 years. The Guardian. https://www.theguardian.com/world/2013b/jul/31/nsa-top-secret-program-online-data

Greenwald G (2013b) XKeyscore: NSA tool collects nearly everything a user does on the internet. The guardian. https://www.theguardian.com/world/2013a/jun/06/nsa-phone-records-verizon-court-order

Greenwald G (2014) Glenn greenwald: how the NSA tampers with US-made internet routers. The guardian

Grimmett JJ (2001) Encryption export controls (CRS report for congress). https://irp.fas.org/crs/RL30273.pdf

Haggerty KD, Ericson RV (2000) The surveillant assemblage. The Br J Sociol. https://doi.org/10.1080/00071310020015280

Hodkowski WA (1997) Future of internet security: how new technologies will shape the internet and affect the law. Santa Clara High Technol Law J 13(1):217–275

Hult FM (2015) Making policy connections across scales using nexus analysis. In: Hult FM, Johnson DC (eds) Research methods in language policy and planning: a practical guide. Wiley, pp 217–223

Isaac M (2019) Zuckerberg plans to Integrate WhatsApp, Instagram and Facebook Messenger. The New York times. https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html

Jordan K, Polk R (2020) The internet "just works": The EARN IT Act threatens that and more | internet society. Internet society. https://www.internetsociety.org/blog/2020/07/the-internet-just-works-the-earn-it-act-threatens-that-and-more/

Kaufmann S (2016) Security through technology? Logic, ambivalence and paradoxes of technologised security. Eur J Secur Res 1(1):77–95. https://doi.org/10.1007/s41125-016-0005-1

Kessler G, Phillips A (2020) Cryptography, passwords, privacy, and the fifth amendment. J Dig Forensics Secur Law 2:78

Kirchgaessner S, Holmes O, Walker S (2021) Pegasus project turns spotlight on spyware firm NSO's ties to Israeli state. The guardian. https://www.theguardian.com/world/2021/jul/20/pegasus-project-turns-spotlight-on-spyware-firm-nso-ties-to-israeli-state

Koops B-J, Kosta E (2018) Looking for some light through the lens of "cryptowar" history: policy options for law enforcement authorities against "going dark." Comput Law Secur Rev 34(4):890–900. https://doi.org/10.1016/j.clsr.2018.06.003

Krawczyk H, Paterson KG, Wee H (2013) On the security of the TLS protocol: a systematic analysis. Annu Cryptol Conf. https://doi.org/10.1007/978-3-642-40041-4_24

Landau S (2015) NSA and dual EC_DRBG: Déjà Vu All over again? Math Intell 37(4):72–83. https://doi.org/10.1007/s00283-015-9543-z

Larson J (2013) Revealed: The NSA's secret campaign to crack, undermine internet security. ProPublica. https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption

LeClair D (2020) New US Bill would require makers of encrypted devices to leave a backdoor. Andriod authority. https://www.androidauthority.com/lawful-access-to-encrypted-data-1132922/

Lyon D (Ed.) (2006) Theorizing surveillance: the panopticon and beyond. In: Theorizing surveillance*:* the panopticon and beyond, Willan Publishing. Doi: https://doi.org/10.1177/009430610703600639

Maurer T, Omanovic E, Wagner B (2014) Uncontrolled global surveillance - updating export controls to the digital age. New America foundation, digitale gesellschaft and privacy international. https://www.newamerica.org/oti/policy-papers/uncontrolled-global-surveillance-updating-export-controls-to-thedigital-age/

Menn J (2013) Exclusive: secret contract tied NSA and security industry pioneer. Reuters, London

Monsees L (2019) Crypto-politics: encryption and democratic practices in the digital era. Routledge, London

Monsees L (2020) Cryptoparties: empowerment in internet security? Internet Policy Rev 9(4):1–19. https://doi.org/10.14763/2020.4.1508

Moore GM (1965) Cramming more components onto integrated circuits With unit cost. Electronics 38(8):114

Murphy CC (2020) The crypto-wars myth: the reality of state access to encrypted communications. Common Law World Rev 49(3–4):245–261. https://doi.org/10.1177/1473779520980556

Olmstead K, Polk R (2020) Latest U.S. 'anti-encryption' bill threatens security of millions. Internet society. https://www.internetsociety.org/blog/2020/07/latest-u-s-anti-encryption-bill-threatens-security-of-millions/

OpenPGP: About (2020) https://www.openpgp.org/about/

Paterson K (2015) Countering cryptographic subversion. post-snowden cryptography workshop. www.isg.rhul.ac.uk/~kp

Pauli R, Sarwary H, Imbusch P, Lukas T (2016) Accepting the rules of the game: institutional rhetorics in legitimizing surveillance. Euro J Secur Res 1(2):115–133. https://doi.org/10.1007/s41125-016-0007-z

Perlroth N, Goel V (2013) Internet firms step up efforts to stop spying. *The* New York Times. https://www.nytimes.com/2013/12/05/technology/internet-firms-step-up-efforts-to-stop-spying.html

Perlroth N, Larson J, Shane S (2013) N.S.A. Able to foil basic safeguards of privacy on web. The New York Times. https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

Pfefferkorn R (2020) The EARN IT act: how to ban end-to-end encryption without actually banning It. Center for Internet and Society. http://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it

Poscher R (2016) Tendencies in public civil security law. Eur J Secur Res 1(1):59–76. https://doi.org/10.1007/s41125-016-0003-3

Reform Governement Surveillance (RSG) (2020) https://www.reformgovernmentsurveillance.com

Riebe T, Haunschild J, Divo F, Lang M, Roitburd G, Franken J, Reuter C (2020) Die Veränderung der Vorratsdatenspeicherung in Europa Datenschutz und Datensicherheit – DuD 44(5):316–321. https://doi.org/10.1007/s11623-020-1275-3

Rich S, Gellmann B (2014) NSA seeks to build quantum computer that could crack most types of encryption. The Washington Post. https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html

Rozenshtein AZ (2018) Surveillance Intermediaries. Stanf Law Rev 70:99–189

Saper N (2013) International cryptography regulation and the global information economy. Northwest J Technol Intellect Prop 11(7):673–688. https://doi.org/10.1109/ICECENG.2011.6057249

Savage C (2020). N.S.A. Phone program cost $100 Million, but produced only two unique leads. The New York Times pp. 3–5. https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html

Schulze M (2017) Clipper meets apple versus FBI—A comparison of the cryptography discourses from 1993 and 2016. Media Commun 5(1):54–62

Schwechter MS (2016) Brief export controls for software companies—what you need to know. BakerHostetler. https://www.bakerlaw.com/webfiles/Litigation/2016/Brief/09-01-2016-Schwechter-Brief.pdf

Shearer J, Gutmann P (1996) Government, cryptography, and the right to privacy. J Univ Comput Sci 2(3):113–146. https://doi.org/10.3217/jucs-002-03-0113

Sircar S (2017) The crypto wars: interpreting the privacy versus national security debate from a standards perspective. https://repository.library.georgetown.edu/bitstream/handle/10822/1043831/Sircar_georgetown_0076M_13737.pdf?sequence=1&isAllowed=y

Southard LS (1997) Securing information technology through cryptography: an analysis of United States policy. Policy Perspect 4(1):43. https://doi.org/10.4079/pp.v4i1.4190

Stieglitz S, Mirbabaie M, Ross B, Neuberger C (2018) Social media analytics—Challenges in topic discovery, data collection, and data preparation. Int J Inf Manage 39:156–168. https://doi.org/10.1016/j.ijinfomgt.2017.12.002

The White House (1993) *White House Annoucement of the Clipper Initiative: Statement by the press secretary*. CSAIL.

Timberg C, Nakashima E (2013) Agreements with private companies protect U.S. access to cables' data for surveillance. The Washington post. https://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html

Timberg C, Soltani A (2013) By cracking cellphone code, NSA has ability to decode private conversations. The Washington Post. https://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html

Timberg C (2013) NSA slide shows surveillance of undersea cables. The Washington Post. NSA slide shows surveillance of undersea cables. https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html

Timberg C (2014) Newest androids will join iPhones in offering default encryption, blocking police. The Washington Post. https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/

U.S. Department of Commerce (2010) Rules and Regulations. Federal Register, 75(122): 36482–36503. https://www.govinfo.gov/content/pkg/FR-2010-06-25/html/2010-15072.htm

U.S. Department of Commerce (2016) U.S. commerce control list (CCL)—cat. 5 Part 2 (pp. 1–11). https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

U.S. Department of Commerce (2020) Encryption and export administration regulations (EAR). https://www.bis.doc.gov/index.php/policy-guidance/encryption

U.S. Department of Commerce, & National Institute of Standards and Technology (1994) Approval of federal information processing standards publication 185, Escrowed encryption standard (EES). Federal register —notices vol. 59(27)

van Hoboken J, Rubinstein I (2014) Privacy and security in the cloud: some realism about technical solutions to transnational surveillance in the post-snowden Era. Maine Law Rev 66(2):488–524

Vella V (2017) Is there a common understanding of dual-use? The case of cryptography. Strateg Trade Rev 3(4):103–122

Wassenaar Arrangement Secretariat (2017) The Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies—List of dual-use goods and technologies and munitions list. Wassenaar Arrangement Secretariat.

Wassenaar Arrangement Secretariat (2021) The Wassenaar Arrangement. https://www.wassenaar.org

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.