COMPUTER LAW & SECURITY REVIEW 34 (2018) 890–900

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark"

*Bert-Jaap Koops**, *Eleni Kosta**

Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, The Netherlands

ARTICLE INFO

Article history:

Keywords:
Encryption
Law enforcement access
Cryptowars
Crypto policy
Backdoors
Decryption orders
Legal hacking

ABSTRACT

As companies and end-users increasingly deploy end-to-end encryption, law enforcement and national security agencies claim they "go dark", i.e. lose in practice the power to legally intercept and gain access to information and communications. This has revived a debate that seemed closed by the late 1990s, namely whether backdoors should be embedded in encryption systems. This paper provides a historical overview of the policy debates surrounding encryption, to identify the potential regulatory options for policy-makers, based on the lessons that can be learned from "cryptowar" history. We discuss the First Cryptowars (1990s, focusing on backdoor schemes), the Interbellum (featuring a rise in powers to order decryption), the Second Cryptowars (2010s, renewed backdoor discussions) and their aftermath: the newly emerging battlefield of legal hacking. The latter can be seen as a condition for the truce with which – for now – the Cryptowars seem to have ended. Cryptowar history teaches us that the two main policy options for decryption by government agencies – ensuring access to keys *ex ante* (backdoors) or *ex post* (decryption orders) – both suffer from fundamental flaws. Therefore, legal hacking powers – if human rights standards are sufficiently taken into account – could be the only realistic policy option to preserve some light in an era of dark communication channels.

1. Introduction

Law-enforcement authorities traditionally have powers of lawful interception, i.e. the statutory-based action of providing access and delivery of a subject's telecommunications and call-associated data to law enforcement agencies, [1] as well to lawfully access stored data, based on national legislation. Obviously the broader the use of encrypted communications, the less potential law enforcement authorities have to benefit from lawful access to information, if they do not have the power or capacity to decrypt the data. In the 1990s, attempts were considered in the US and elsewhere to ensure the presence of backdoors in software products for national

* Corresponding authors: Bert-Jaap Koops & Eleni Kosta, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, P.O. Box 90153, 5000 LE Tilburg, The Netherlands.

E-mail addresses: E.J.Koops@uvt.nl (B.-J. Koops), E.Kosta@uvt.nl (E. Kosta).

[1] Council Resolution of 17 January 1995 on the lawful interception of telecommunications, Official Journal C 329, 04/11/1996, p. 1-6.

https://doi.org/10.1016/j.clsr.2018.06.003

security and law enforcement agencies. This sparked a heated debate between the government and governmental agencies on the one hand, and companies and the cryptographic community on the other, commonly known as the "Cryptowars".[2] The ability of national security agencies and law enforcement authorities to access private communications and information is generally acknowledged in all democratic societies. However, compromising the security of software systems and communications to that end was considered highly disproportionate to the confidentiality of communications and the protection of rights of individuals, as it was opening a security backdoor exposing the systems to malicious attacks.

As a response to the Cryptowars debate, in 1997, the OECD published Guidelines for Cryptography Policy,[3] without however offering any concrete solutions. Principle 2 of the guidelines recognises the rights of users "to choose any cryptographic method, subject to applicable law".[4] However, the guidelines do not take a clear stance on what applicable law could or should look like, leaving it up to the national regulators to solve this complex issue. The explanatory text of Principle 2 clarifies on this point that "Government controls on cryptographic methods should be no more than are essential to the discharge of government responsibilities and should respect user choice to the greatest extent possible".[5] Principles 5 and 6 remind the participants in the debate to consider both key issues: principle 5 is dedicated to protection of privacy and personal data, while principle 6 refers to lawful access. The former calls for the respect of the "fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, […] in national cryptography policies and in the implementation and use of cryptographic methods",[6] while the latter recognises that "[n]ational cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible".[7] Reconciliation of these two principles remains still an unresolved puzzle.

Soon after the adoption of the OECD cryptography guidelines, Steve Saxby, the founding editor of *Computer Law and Security Review* (founded in 1985 as *Computer Law and Security Report*), in his editorial entitled "Electronic commerce a step closer following adoption of OECD cryptography guidelines", highlighted the importance of the guidelines and the importance of policy responses for state governments.[8] Since then he has been systematically dealing with issues relating to cryptography in his editorials, and the *Computer Law and Security Report/Review* has hosted hundreds of academic papers examining the legal and policy debates surrounding cryptography from both technical and legal perspectives. This demonstrates not only the persistence of the debate on what is nowadays also referred to as the "going dark" problem, and the associated dilemmas for policy-makers for whom no silver bullets are available (or in this case, silver parachute flares). It also demonstrates the outstanding position that the *Computer Law and Security Review*, under Saxby's unwavering guidance, has taken up at the forefront of the academic and policy debates surrounding the most pressing regulatory issues in the information society. A historic overview of the Cryptowars and the dilemmas associated with "going dark" is therefore also an eminently suitable topic to present in the celebratory 200th edition of this leading journal.

Encryption can be used by various actors and at various stages of a communication process: (i) encryption that is centrally managed by the service provider, in which case the provider manages the cryptographic keys, (ii) transport encryption by the provider, which protects the interception of information and communications while in transit, (iii) end-to-end encryption by software providers who offer a communications option (e.g., Skype, or chatting in an online game) on top of the channel managed by the traditional telco companies (the "mere conduit" providers), and (iv) end-to-end encryption by end users. In the former two cases, the transport provider is capable of decryption, and these two situations have been traditionally more regulated, requiring the transport providers to decrypt when ordered by law enforcement authorities, usually following a court order. In contrast, the third and fourth cases, the telco companies responsible for the channel have no capacity to decrypt communications; these types of encryption therefore raise the most important challenges for law enforcement authorities in seeing their channels darkening. Traditional lawful interception capabilities will most likely be sufficient to overcome encryption in the first situation. Similarly, in the second situation, law enforcement authorities may have the opportunity to request access to the data after the transit when they are actually stored, arguably under less secure conditions. The last two cases of end-to-end encryption however raise significant concerns, as the telecommunications provider cannot deliver something they do not have, i.e. the cryptographic keys.

Following the Snowden disclosures, which revealed an NSA decryption programme of a large scale, private companies and individuals alike are making gradually more use of encryption tools and predominantly of end-to-end encryption.[9] All these factors have led national security agencies and law enforcement authorities to claim that they "go dark", i.e. that they lose

[2] For an overview of the debate and policy options considered in the 1990s, see Lance J. Hoffman (ed.), *Building in Big Brother. The Cryptographic Policy Debate* (New York: Springer, 1995); Kenneth W. Dam and Herbert S. Lin (eds), National Research Council, *Cryptography's Role In Securing the Information Society* (Washington, D.C.: National Academy Press, 1996); Bert-Jaap Koops, *The Crypto Controversy. A Key Conflict in the Information Society* (The Hague: Kluwer Law International 1999).

[3] OECD, Recommendation of the Council concerning Guidelines for Cryptography Policy (1997), https://legalinstruments.oecd.org/en/instruments/115.

[4] *Ibid*., principle 2.

[5] *Ibid*., principle 2, explanatory text.

[6] *Ibid*., principle 5.

[7] *Ibid*., principle 6.

[8] Stephen Saxby, Editorial: Electronic commerce a step closer following adoption of OECD cryptography guidelines, CLSR [1997] 13(3), 150.

[9] Joris van Hoboken and Ira Rubinstein, 'Privacy and security in the cloud: Some realism about technical solutions to transnational surveillance in the post-Snowden era' (2014) 66 *Maine Law Review* 496.