Key disclosure law

Key disclosure laws, also known as **mandatory key disclosure**, is legislation that requires individuals to surrender cryptographic keys to law enforcement. The purpose is to allow access to material for confiscation or digital forensics purposes and use it either as evidence in a court of law or to enforce national security interests. Similarly, **mandatory decryption** laws force owners of encrypted data to supply decrypted data to law enforcement.[1]

Nations vary widely in the specifics of how they implement key disclosure laws. Some, such as Australia, give law enforcement wide-ranging power to compel assistance in decrypting data from any party. Some, such as Belgium, concerned with self-incrimination, only allow law enforcement to compel assistance from non-suspects. Some require only specific third parties such as telecommunications carriers, certification providers, or maintainers of encryption services to provide assistance with decryption. In all cases, a warrant is generally required.

Theory and countermeasures

Mandatory decryption is technically a weaker requirement than key disclosure, since it is possible in some cryptosystems to prove that a message has been decrypted correctly without revealing the key. For example, using RSA public-key encryption, one can verify given the message (plaintext), the encrypted message (ciphertext), and the public key of the recipient that the message is correct by merely re-encrypting it and comparing the result to the encrypted message. Such a scheme is called *undeniable*, since once the government has validated the message they cannot deny that it is the correct decrypted message.[2]

As a countermeasure to key disclosure laws, some personal privacy products such as BestCrypt, FreeOTFE, and TrueCrypt have begun incorporating deniable encryption technology, which enable a single piece of encrypted data to be decrypted in two or more different ways, creating plausible deniability.[3][4] Another alternative is steganography, which hides encrypted data inside of benign data so that it is more difficult to identify in the first place.

A problematic aspect of key disclosure is that it leads to a total compromise of all data encrypted using that key in the past or future; time-limited encryption schemes such as those of Desmedt et al.[2] allow decryption only for a limited time period.

Criticism and alternatives

Critics of key disclosure laws view them as compromising information privacy,[1] by revealing personal information that may not be pertinent to the crime under investigation, as well as violating the right against self-incrimination and more generally the right to silence, in nations which respect these rights. In some cases, it may be impossible to decrypt the data because the key has been lost, forgotten or revoked, or because the data is actually random data which cannot be effectively distinguished from encrypted data.

A proactive alternative to key disclosure law is key escrow law, where the government holds in escrow a copy of all cryptographic keys in use, but is only permitted to use them if an appropriate warrant is issued. Key escrow systems face difficult technical issues and are subject to many of the same criticisms as key disclosure law; they avoid some issues like lost keys, while introducing new issues such as the risk of accidental disclosure of large numbers of keys, theft of the keys by hackers or abuse of power by government employees with access to the keys. It would also be

nearly impossible to prevent the government from secretly using the key database to aid mass surveillance efforts such as those exposed by Edward Snowden.[1] The ambiguous term *key recovery* is applied to both types of systems.

Legislation by nation

This list shows only nations where laws or cases are known about this topic.

Antigua and Barbuda

The Computer Misuse Bill, 2006, Article 21(5)(c), if enacted, would allow police with a warrant to demand and use decryption keys. Failure to comply may incur "a fine of fifteen thousand [East Caribbean] dollars" and/or "imprisonment for two years."[5]

Australia

The Cybercrime Act 2001 No. 161, Items 12 and 28 grant police with a magistrate's order the wide-ranging power to require "a specified person to provide any information or assistance that is reasonable and necessary to allow the officer to "access computer data that is "evidential material"; this is understood to include mandatory decryption. Failing to comply carries a penalty of 6 months' imprisonment. Electronic Frontiers Australia calls the provision "alarming" and "contrary to the common law privilege against self-incrimination."[6]

The Crimes Act 1914, 3LA(5) "A person commits an offence if the person fails to comply with the order. Penalty for contravention of this subsection: Imprisonment for 2 years."[7]

Belgium

The *Loi du 28 novembre 2000 relative à la criminalité informatique* (Law on computer crime of 28 November 2000), Article 9 allows a judge to order the authorities to search the computer systems and telecommunications providers to provide assistance to law enforcement, including mandatory decryption, and to keep their assistance secret; but this action cannot be taken against suspects or their families.[8][9] Failure to comply is punishable by 6 months to 1 year in jail and/or a fine of 130 to 100,000 euros.

Cambodia

Cambodia promulgated its Law on Electronic Commerce on 2 November 2019, after passage through legislature and receiving consent from the monarch, becoming the last among ASEAN states to adopt a domestic law governing electronic commerce.[10] Article 43 of the statute prohibits any encryption of evidence in the form of data that could lead to an indictment, or any evidence in an electronic system that relates to an offense.[11] This statutory obligation may imply that authorities could order decryption of any data implicated in an investigation.[12] While remaining untested in courts, this obligation actively contradicts an accused person's procedural right against self-incrimination as provided under Article 143 of the Code of Criminal Procedure.[13]

Canada

In Canada key disclosure is covered under the *Canadian Charter of Rights and Freedoms* section 11(c) which states "any person charged with an offence has the right not to be compelled to be a witness in proceedings against that person in respect of the offence;"[14] and protects the rights of individuals that are both citizens and non-citizens of Canada as long as they are physically present in Canada.[15]

In a 2010 Quebec Court of Appeal case the court stated that a password compelled from an individual by law enforcement "is inadmissible and that renders the subsequent seizure of the data unreasonable. In short, even had the seizure been preceded by judicial authorization, the law will not allow an order to be joined compelling the respondent to self-incriminate."[16]

In a 2019 Ontario court case (R v. Shergill (https://www.canlii.org/en/on/oncj/doc/2019/2019oncj54/2019oncj54.html)), the defendant was initially ordered to provide the password to unlock his phone. However, the judge concluded that providing a password would be tantamount to self-incrimination by testifying against oneself. As a result, the defendant was not compelled to provide his password.[17]

Czech Republic

In the Czech Republic there is no law specifying obligation to issue keys or passwords.[18] Law provides protecting against self-incrimination, including lack of penalization for refusing to answer any question which would enable law enforcement agencies to obtain access to potential evidence, which could be used against testifying person.[19]

Finland

The Coercive Measures Act (*Pakkokeinolaki*) 2011/806 section 8 paragraph 23[20] requires the system owner, its administrator, or a specified person to surrender the necessary "passwords and other such information" in order to provide access to information stored on an information system. The suspect and some other persons specified in section 7 paragraph 3 that cannot otherwise be called as witnesses are exempt from this requirement.

France

Loi n^{o} 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, article 30 (Law #2001-1062 of 15 November 2001 on Community Safety) allows a judge or prosecutor to compel any qualified person to decrypt or surrender keys to make available any information encountered in the course of an investigation. Failure to comply incurs three years of jail time and a fine of €45,000; if the compliance would have prevented or mitigated a crime, the penalty increases to five years of jail time and €75,000.[21]

Germany

The German Code of Criminal Procedure grants a suspect the right to deny cooperation in an investigation that may lead to incriminating information to be revealed about themselves. For private usage is no legal basis that would compel a suspect to hand over any kind of cryptographic key due to this *nemo tenetur* principle.[22]

There are different laws (tax, crime, etc.) stating that companies must ensure this data is readable by the government. This includes the need to disclose the keys or unencrypted content as and when required.

Iceland

In Iceland there is no law specifying obligation to issue keys or passwords.

India

Section 69 of the Information Technology Act, as amended by the Information Technology (Amendment) Act, 2008, empowers the central and state governments to compel assistance from any "subscriber or intermediary or any person in charge of the computer resource" in decrypting information.[23][24] Failure to comply is punishable by up to seven years' imprisonment and/or a fine.

Ireland

Section 7(4)(b) of the Criminal Justice (Offences Relating to Information Systems) Act 2017 allows a member of the Garda Síochána or other persons as deemed necessary (via a search warrant issued by a judge of the District Court (Section 7(1))) to demand the disclosure of a password to operate a computer and any decryption keys required to access the information contained therein.[25]

> 7(4) A member acting under the authority of a search warrant under this section may—
>
> (a) operate any computer at the place that is being searched or cause any such computer to be operated by a person accompanying the member for that purpose, and
>
> (b) require any person at that place who appears to the member to have lawful access to the information in any such computer—
>
> (i) to give to the member any password necessary to operate it and any encryption key or code necessary to unencrypt the information accessible by the computer, immediate data destruction
>
> (ii) otherwise to enable the member to examine the information accessible by the computer in a form in which the information is visible and legible, or
>
> (iii) to produce the information in a form in which it can be removed and in which it is, or can be made, visible and legible.

New Zealand

As of 2016 New Zealand Customs was seeking power to compel key disclosure.[26] Although New Zealand may not have a key disclosure law, they have since enforced penalties against travelers unwilling to unlock mobile devices when compelled to do so by officials.[27]

Poland

In relatively few known cases in which police or prosecutor requested cryptographic keys from those formally accused and these requests were not fulfilled, no further consequences were imposed on the accused. There's no specific law in this matter, as e.g. in the UK. It is generally assumed that the Polish Criminal Procedure Code (Kodeks Postępowania Karnego Dz.U. 1997 nr 89 poz. 555.) provides means of protecting against self-incrimination, including lack of penalization for refusing to answer any question which would enable law enforcement agencies to obtain access to potential evidence, which could be used against testifying person.[28]

South Africa

Under the RICA Act of 2002, refusal to disclose a cryptographic key in one's possession could result in a fine up to ZAR 2 million or up to 10 years' imprisonment. This requires a judge to issue a decryption direction to a person believed to hold the key.

Spain

Spain's Criminal Procedure Law grants suspects rights against self-incrimination,[29] and this would prevent the suspect from being compelled to reveal passwords.[30] However, a judge may order third parties to collaborate with any criminal investigation, including revealing decryption keys, where possible.[31]

Sweden

There are currently no laws that force the disclosure of cryptographic keys. However, there is legislation proposed on the basis that the Council of Europe has already adopted a convention on cyber-crime related to this issue. The proposed legislation would allow police to require an individual to disclose information, such as passwords and cryptographic keys, during searches. The proposal has been introduced to make it easier for police and prosecutors. The proposal has been criticized by the Swedish Data Protection Authority.[32][33]

Switzerland

In Switzerland there is no law specifying obligation to issue keys or passwords.[34]

The Netherlands

Article 125k of the Wetboek van Strafvordering allows investigators with a warrant to access information carriers and networked systems. The same article allows the district attorney and similar officers of the court to order persons who know how to access those systems to share their knowledge in the investigation, including any knowledge of encryption of data on information carriers. However, such an order may not be given to the suspect under investigation.[35]

United Kingdom

The Regulation of Investigatory Powers Act 2000 (RIPA), Part III, activated by ministerial order in October 2007,[36] requires persons to decrypt information and/or supply keys to government representatives to decrypt information without a court order. Failure to disclose carries a maximum penalty of two years in jail, or five years in the cases of national security or child indecency. The provision was first used against animal rights activists in November 2007,[37] and at least three people have been prosecuted and convicted for refusing to surrender their encryption keys,[38] one of whom was sentenced to 13 months' imprisonment.[39] Even politicians responsible for the law have voiced concerns that its broad application may be problematic.[40]

In 2017, schedule 7 of the Terrorism Act 2000 was used to charge Muhammad Rabbani with "wilfully obstructing or seeking to frustrate a search examination" after allegedly refusing to disclose passwords.[41] He was later convicted.[42]

In 2018, Stephen-Alan Nicholson, the prime suspect in a murder case, was charged with refusing to provide his Facebook password to police.[43]

United States

The Fifth Amendment to the United States Constitution protects witnesses from being forced to incriminate themselves, and there is currently no law regarding key disclosure in the United States.[44] However, the federal case *In re Boucher* may be influential as case law. In this case, a man's laptop was inspected by customs agents and child pornography was discovered. The device was seized and powered-down, at which point disk encryption technology made the evidence unavailable. The judge held that it was a foregone conclusion that the content exists since it had already been seen by the customs agents, Boucher's encryption password "adds little or nothing to the sum total of the Government's information about the existence and location of files that may contain incriminating information."[45][46]

In another case, a district court judge ordered a Colorado woman to decrypt her laptop so prosecutors can use the files against her in a criminal case: "I conclude that the Fifth Amendment is not implicated by requiring production of the unencrypted contents of the Toshiba Satellite M305 laptop computer," Colorado U.S. District Judge Robert Blackburn ruled on January 23, 2012.[47] In *Commonwealth v. Gelfgatt*,[48] the court ordered a suspect to decrypt his computer, citing exception to Fifth Amendment can be invoked because "*an act of production does not involve testimonial communication where the facts conveyed already are known to the government...*".[49]

However, in *United States v. Doe*, the United States Court of Appeals for the Eleventh Circuit ruled on 24 February 2012 that forcing the decryption of one's laptop violates the Fifth Amendment.[50][51]

The Federal Bureau of Investigation may also issue national security letters that require the disclosure of keys for investigative purposes.[52] One company, Lavabit, chose to shut down rather than surrender its master private keys due to the government wanting to spy on Edward

Snowden's emails.

Since the summer of 2015, cases have been fought between major tech companies such as Apple over the regulation of encryption with government agencies asking for access to private encrypted information for law enforcement purposes. A technical report was written and published by MIT Computer Science and Artificial Intelligence Laboratory, where Ronald Rivest, an inventor of RSA, and Harold Abelson, a computer science professor at MIT with others, explain the technical difficulties, including security issues that arise from the regulation of encryption or by making a key available to a third party for purposes of decrypting any possible encrypted information. The report lists scenarios and raises questions for policy makers. It also asks for more technical details if the request for regulating encryption is to be pursued further.[53]

In 2019, the Pennsylvania Supreme Court, in a ruling that only controls for that state's law, held that a suspect in a child pornography case could not be compelled to reveal his password, despite telling the police "We both know what's on there."[54]

See also

- Deniable encryption
- FBI–Apple encryption dispute
- Secret sharing
- Rubber-hose cryptanalysis
- Crypto Wars

References

1. Ranger, Steve (24 March 2015). "The undercover war on your internet secrets: How online surveillance cracked our trust in the web" (https://web.archive.org/web/20160612190952/http://www.techrepublic.com/article/the-undercover-war-on-your-internet-secrets-how-online-surveillance-cracked-our-trust-in-the-web/). TechRepublic. Archived from the original (https://www.techrepublic.com/article/the-undercover-war-on-your-internet-secrets-how-online-surveillance-cracked-our-trust-in-the-web/) on 2016-06-12. Retrieved 2016-06-12.
2. Desmedt, Yvo and Burmester, Mike and Seberry, Jennifer. Equitability in Retroactive Data Confiscation versus Proactive Key Escrow. Florida State University Department of Computer Science 206 Love Building FL 32306-4530 Tallahassee USA. Lecture Notes in Computer Science: Public Key Cryptography, pp.277-286. 2001. (Postscript) (http://www.cs.fsu.edu/~burmeste/ripsubmit.ps), (Postscript 2) (http://www.uow.edu.au/~jennie/WEB/pkc2001.ps) Archived (https://web.archive.org/web/20170830010905/http://www.uow.edu.au/~jennie/WEB/pkc2001.ps) 2017-08-30 at the Wayback Machine
3. Plausible Deniability (http://www.freeotfe.org/docs/Main/plausible_deniability.htm)
4. TrueCrypt - Hidden Volume (https://archive.today/20120914151319/http://www.truecrypt.org/hiddenvolume)
5. "Antigua and Barbuda: The Computer Misuse Bill, 2006" (https://web.archive.org/web/20110706071016/http://www.laws.gov.ag/bills/2006/computer-misuse-bill-2006.pdf) (PDF). Archived from the original (http://www.laws.gov.ag/bills/2006/computer-misuse-bill-2006.pdf) (PDF) on 2011-07-06. Retrieved 2010-11-09.
6. Electronic Frontiers Australia. Privacy Laws in Australia: Security / Cybercrime (http://www.efa.org.au/Issues/Privacy/security.html#ccb01). Retrieved 2010 November 8.
7. AG. "Crimes Act 1914" (http://www.comlaw.gov.au/Details/C2015C00111/Html/Volume_1#_Toc415554770). *www.comlaw.gov.au*. Retrieved 2016-04-30.

8. Loi du 28 novembre 2000 relative à la criminalité informatique: Article 9 (https://web.archive.org/web/20080716214402/http://cwisdb.kuleuven.be/pisa/fr/jur/infocrimewet.htm). 2000 November 28. Retrieved 2010 November 9. (The investigating judge may order any appropriate person to put the computer system into operation himself or, as the case may be, to search for, make available, copy, render inaccessible or remove the relevant data stored, processed or transmitted by that system, in the form he has requested. Such persons shall be obliged to comply with such requests to the extent of their ability.)
9. Code d'instruction criminelle. Livre II, titre I, Art. 156. (http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?DETAIL=1808111930%2FF&caller=list&row_id=1&numero=7&rech=9&cn=1808111930&table_name=LOI&nm=1808111901&la=F&dt=CODE+D%27INSTRUCTION+CRIMINELLE&language=fr&fromtab=loi_all&sql=dt+contains++%27CODE%27%26+%27D%27%26+%27INSTRUCTION%27%26+%27CRIMINELLE%27and+actif+%3D+%27Y%27#Art.156) 1808 November 19. Retrieved 2010 November 9. (*in French*)
10. Cohen, Jay; Bunthan, Pichrotanak (2020-03-02). "What Cambodia's New Law on Electronic Commerce Means for Business" (https://www.lexology.com/library/detail.aspx?g=442bd243-f5af-4002-a3b4-b4d8c4e24f39). *Lexology*. Retrieved 2021-07-22.
11. "Law on Electronic Commerce (Khmer)" (https://www.ocm.gov.kh/wp-content/uploads/2019/11/%E1%9E%85%E1%9F%92%E1%9E%94%E1%9E%B6%E1%9E%94%E1%9F%8B%E1%9E%9F%E1%9F%92%E1%9E%8F%E1%9E%B8%E1%9E%96%E1%9E%B8%E1%9E%96%E1%9E%B6%E1%9E%8E%E1%9E%B7%E1%9E%87%E1%9F%92%E1%9E%87%E1%9E%80%E1%9E%98%E1%9F%92%E1%9E%98%E1%9E%8F%E1%9E%B6%E1%9E%98%E1%9E%94%E1%9F%92%E1%9E%9A%E1%9E%96%E1%9F%90%E1%9E%93%E1%9F%92%E1%9E%92%E1%9E%A2%E1%9F%81%E1%9E%A1%E1%9E%B7%E1%9E%85%E1%9E%8F%E1%9F%92%E1%9E%9A%E1%9E%BC%E1%9E%93%E1%9E%B7%E1%9E%80.pdf) (PDF). *Office of the Council of Ministers (Cambodia)*. Retrieved 22 July 2021.
12. Cohen, Jay (2020-08-17). "Cambodia - Data Protection Overview" (https://www.dataguidance.com/notes/cambodia-data-protection-overview). *DataGuidance*. Retrieved 2021-07-22.
13. "Cambodia Annotated Code of Criminal Procedure | OHCHR" (https://cambodia.ohchr.org/en/rule-of-law/cambodia-annotated-code-criminal-procedure). *cambodia.ohchr.org*. Retrieved 2021-07-22.
14. Your Guide to the Canadian Charter of Rights and Freedoms (https://www.canada.ca/en/canadian-heritage/services/how-rights-protected/guide-canadian-charter-rights-freedoms.html#section11). Government of Canada. Last modified 2017 October 24. Retrieved 2018 January 29.
15. Singh Case (https://www.thecanadianencyclopedia.ca/en/article/singh-case/). The Canadian Encyclopedia. Last modified 2017 August 6. Retrieved 2018 January 29.
16. R. c. Boudreau-Fontaine, 2010 QCCA 1108 (CanLII) (https://www.canlii.org/en/qc/qcca/doc/2010/2010qcca1108/2010qcca1108.html). Quebec Court of Appeal. 2010 June 9. Retrieved 2018 January 29.
17. "COMMENTARY: Can Canadian courts force you to reveal your password? The jury is still out" (https://globalnews.ca/news/5310901/canada-privacy-passwords-law/). *Global News*. Retrieved 2020-05-23.
18. "Zákaz donucování k sebeobviňování" (http://www.mvcr.cz/clanek/4-2009-zakaz-donucovani-k-sebeobvinovani-nemo-tenetur-se-ipsum-accusare.aspx) (in Czech). Retrieved 2016-05-06.
19. "VÝJIMKY Z POVINNOSTI VYPOVÍDAT JAKO SVĚDEK V TRESTNÍM ŘÍZENÍ" (http://www.epravo.cz/top/clanky/vyjimky-z-povinnosti-vypovidat-jako-svedek-v-trestnim-rizeni-17716.html) (in Czech). Retrieved 2016-05-06.
20. "Coercive Measures Act (Pakkokeinolaki)" (http://www.finlex.fi/fi/laki/ajantasa/2011/20110806#a806-2011) (in Finnish). Retrieved 2016-04-30.
21. Articles 30–31, *loi n^{o} 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne* (http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052) (in French)

22. Government Access to Encrypted Communications: Germany (https://www.loc.gov/law/help/encrypted-communications/germany.php#encryption-communications). 2016 October 01. Retrieved 2017 December 6.
23. Information Technology (Amended) Act, 2008 (http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf) (PDF); Government of India – Ministry of Law, Justice and Company Affairs (Legislative Department); **XI** (69) pp. 27–8.
24. Paper – 6 : Information Systems Control and Audit (http://220.227.161.86/18962sm_finalnew_isca_cp10.pdf) Archived (https://web.archive.org/web/20120711085016/http://220.227.161.86/18962sm_finalnew_isca_cp10.pdf) 2012-07-11 at the Wayback Machine (PDF) **10** pp. 42–3. Study Material - Final (New) (http://www.icai.org/post.html?post_id=5777) The Institute of Chartered Accountants of India.
25. (eISB), electronic Irish Statute Book. "Search warrant" (http://www.irishstatutebook.ie/eli/2017/act/11/section/7/enacted/en/html#sec7). *www.irishstatutebook.ie*. Retrieved 2018-03-23.
26. "Customs downplays password plan" (http://www.stuff.co.nz/technology/digital-living/67449940/customs-downplays-password-plan). *Stuff*. 19 March 2015. Retrieved 2016-04-30.
27. Graham-Mclay, Charlotte (2 October 2018). "Fork Over Passwords or Pay the Price, New Zealand Tells Travelers" (https://www.nytimes.com/2018/10/02/world/asia/new-zealand-passwords-devices.html). *The New York Times*. Retrieved 2019-12-24.
28. Webhosting.pl - W jaki sposób służby mogą uzyskać dostęp do zaszyfrowanych danych (https://archive.today/20130706153423/http://webhosting.pl/W.jaki.sposob.sluzby.moga.uzyskac.dostep.do.zaszyfrowanych.danych)
29. "BOE - Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, artículo 520" (https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036&p=20201120&tn=1#a520). *Boletín Oficial del Estado*. 2020-11-20. Retrieved 2021-03-06.
30. "La contraseña del móvil, el cómplice más leal del delincuente" (https://www.lavanguardia.com/tecnologia/20170619/423494281614/contrasena-movil-policia-delito.html). *La Vanguardia* (in Spanish). 2017-06-18. Retrieved 2021-03-06.
31. "BOE - Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registro de dispositivos y equipos informáticos" (https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4244). *Boletín Oficial del Estado*. 2019-03-22. Retrieved 2021-03-06.
32. "DI kritiserar nya it-regler" (http://www.publikt.se/artikel/di-kritiserar-nya-it-regler-46346). *Publikt* (in Swedish). 2013-09-26. Retrieved 2016-04-30.
33. "Remiss av betänkandet Europarådets konvention om it - relaterad brottslighet (SOU 2013:39)" (https://web.archive.org/web/20140522001655/http://www.datainspektionen.se/Documents/remissvar/2013-09-25-konvention-it-brottslighet.pdf) (PDF) (in Swedish). Archived from the original (http://www.datainspektionen.se/Documents/remissvar/2013-09-25-konvention-it-brottslighet.pdf) (PDF) on 2014-05-22.
34. "Global Partners Digital, select Switzerland in the drop down menu" (https://www.gp-digital.org/world-map-of-encryption/). *gp-digital.org*. Retrieved 2019-04-01.
35. "wetten.nl - Regeling - Wetboek van Strafvordering - BWBR0001903" (http://wetten.overheid.nl/BWBR0001903/EersteBoek/TitelIV/Zevendeafdeling/Artikel125k/geldigheidsdatum_12-01-2015). *wetten.overheid.nl*. Retrieved 2016-04-30.
36. Kirk, Jeremy (October 1, 2007). "Contested UK encryption disclosure law takes effect" (https://www.washingtonpost.com/wp-dyn/content/article/2007/10/01/AR2007100100511.html). *Washington Post*. PC World. Retrieved 2009-01-05.
37. Ward, Mark (2007-11-20). "Campaigners hit by decryption law" (http://news.bbc.co.uk/1/hi/technology/7102180.stm). *BBC News*. Retrieved 2009-01-05.
38. Oates, John (6 October 2010). "Youth jailed for not handing over encryption password" (https://www.theregister.co.uk/2010/10/06/jail_password_ripa/). *The Register*.
39. Williams, Christopher (24 November 2009). "UK jails schizophrenic for refusal to decrypt files" (https://www.theregister.co.uk/2009/11/24/ripa_jfl). *The Register*.

40. "How Refusing to Hand over Your Passwords Can Land You in Jail" (https://motherboard.vice.com/en_us/article/wnjgdq/how-refusing-to-hand-over-your-passwords-can-land-you-in-jail).
41. "Cage director charged under Terrorism Act after failing to hand over passwords" (https://www.theguardian.com/uk-news/2017/may/17/cage-campaign-group-director-muhammed-rabbani-charged-under-terrorism-act). *The Guardian*.
42. "Man found guilty under UK terrorism laws after refusing to reveal passwords" (http://uk.reuters.com/article/uk-britain-security-password/man-found-guilty-under-uk-terrorism-laws-after-refusing-to-reveal-passwords-idUKKCN1C02PE). *Reuters*.
43. "Suspect in Lucy McHugh murder remanded in custody for failing to provide Facebook password to detectives" (https://www.independent.co.uk/news/uk/home-news/lucy-mchugh-murder-facebook-southampton-woods-stabbing-death-a8471566.html). *Independent.co.uk*. 31 July 2018.
44. Varma, Corey (28 July 2015). "Encryption vs. Fifth Amendment" (http://www.coreyvarma.com/2015/07/encryption-vs-fifth-amendment/). *www.coreyvarma.com*. Retrieved July 28, 2015.
45. "In re Grand Jury Subpoena to Sebastien Boucher, Memorandum of Decision" (https://web.archive.org/web/20140716161430/http://www.volokh.com/files/Boucher.pdf) (PDF). *The Volokh Conspiracy*. February 19, 2009. Archived from the original (http://volokh.com/files/BoucherDCT.1.pdf) (PDF) on July 16, 2014. Retrieved 2009-08-29.
46. McCullagh, Declan (December 14, 2007). "Judge: Man can't be forced to divulge encryption passphrase" (https://www.cnet.com/news/judge-man-cant-be-forced-to-divulge-encryption-passphrase/). CNET. Retrieved October 19, 2014.
47. Kravets, David (January 23, 2012). "Judge Orders Defendant to Decrypt Laptop" (https://www.wired.com/threatlevel/2012/01/judge-orders-laptop-decryption/). WIRED.
48. Commonwealth v. Gelfgatt (https://scholar.google.com/scholar_case?q=GELFGATT&hl=en&as_sdt=2006&case=13313310379620456644&scilh=0) (Report). Vol. 468. Supreme Judicial Court of Massachusetts. June 25, 2014. p. 512. Retrieved October 19, 2014.
49. Farivar, Cyrus (June 26, 2014). "Massachusetts high court orders suspect to decrypt his computers" (https://arstechnica.com/tech-policy/2014/06/massachusetts-high-court-orders-suspect-to-decrypt-his-computers/). Ars Technica. Retrieved October 19, 2014.
50. Hofmann, Marcia; Fakhoury, Hanni (February 24, 2012). "Appeals Court Upholds Constitutional Right Against Forced Decryption" (https://www.eff.org/press/releases/appeals-court-upholds-constitutional-right-against-forced-decryption). Electronic Frontier Foundation. Retrieved October 19, 2014.
51. Lee, Timothy B. (February 25, 2012). "Appeals court: Fifth Amendment protections can apply to encrypted hard drives" (https://arstechnica.com/tech-policy/2012/02/appeals-court-fifth-amendment-protections-can-apply-to-encrypted-hard-drives/). Ars Technica. Retrieved October 19, 2014.
52. "Lavabit appeals contempt of court ruling surrounding handover of SSL keys" (https://nakedsecurity.sophos.com/2014/01/29/lavabit-appeals-contempt-of-court-ruling-surrounding-handover-of-ssl-keys/). *Naked Security*. 2014-01-29. Retrieved 2016-04-30.
53. *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communication* (https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf) (PDF). *MIT Computer Science and Artificial Intelligence Laboratory* (Technical report). 6 July 2015.
54. Goodin, Dan (November 23, 2019). "Suspect can't be compelled to reveal "64-character" password, court rules" (https://arstechnica.com/tech-policy/2019/11/police-cant-force-child-porn-suspect-to-reveal-his-password-court-rules/). Ars Technica. Retrieved April 26, 2020.

Further reading

- Bert-Jaap Koops. Bert-Jaap Koops homepage (https://web.archive.org/web/20110517045207/http://rechten.uvt.nl/koops/index.htm): Crypto Law Survey: Overview per country (https://web.arc

hive.org/web/20101028103302/http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM). Version 26.0. Universiteit van Tilburg. July 2010.
- Stephen Mason, gen ed, Electronic Evidence (3rd edn, LexisNexis Butterworths, 2012) Chapter 6 Encrypted data
- Palfreyman, Brendan M. (2009). "Lessons from the British and American Approaches to Compelled Decryption". *Brooklyn Law Review*. **75** (1): 345.
- Fakhoury, Hanni (2012). "A combination or a key? The Fifth Amendment and privilege against compelled decryption" (http://www.deaeslr.org/2012.html). *Digital Evidence and Electronic Signature Law Review*. **9**: 81–87.
- List of legal case studies (http://scienceblogs.de/klausis-krypto-kolumne/when-encryption-baffles-the-police-a-collection-of-cases/)
