**Talking in the Dark: Rules to facilitate open debate about lawful access to strongly encrypted information**

**Abstract**

Strong encryption can prevent anybody from accessing user data, including the technology companies responsible for its implementation. As strong encryption technology has become increasingly prevalent, law enforcement agencies have sought legislation to secure continued lawful access to the data affected. Following analysis of the encryption debates in the United States and the United Kingdom, this article will propose three rules that governments should follow to facilitate open debate and prevent the implementation of unsafe lawful access solutions. Firstly, we will provide context on current encryption policy. Secondly, it will be shown that continuous open debate must be facilitated in order to prevent the implementation of unsafe lawful access solutions. Finally, it will be argued that governments should be held to three rules when engaging in debate about lawful access: legislation governing lawful access must state clearly on its face whether decryption can be mandated; the encryption debate must not be oversimplified or reduced to emotive examples in order to secure public support for unsafe solutions; and safeguards on warrants must not be conflated with safeguards on lawful access mechanisms in order to suggest that solutions are safer than is actually the case.

*Key words: Lawful access, going dark, strong encryption, end-to-end encryption, device encryption, investigatory powers*

**1: Background on current encryption policy**

**1.1: Introduction.**

Technologies such as end-to-end encryption and device encryption strongly encrypt user data so that no third parties, including the technology companies responsible for their implementation, hold the decryption keys necessary to access a user’s communications as plaintext. As strong encryption has become more prevalent in mainstream technology, this inability to access user data has increasingly prevented law enforcement agencies from surveilling digital communications, a problem that the Federal Bureau of Investigation has christened *going dark*.[[1]](#footnote-1) Law enforcement agencies have argued that technology companies must alter their secure systems to provide mechanisms whereby they may lawfully access strongly encrypted data as plaintext.[[2]](#footnote-2) In response, technology companies and civil society groups have argued that facilitating lawful access would compromise the security of systems and offer no meaningful benefit in the prevention of crime.[[3]](#footnote-3) These groups contend that lawful access mechanisms could be exploited by malicious actors and that criminals may deploy alternative software in order to continue to avoid surveillance. Traditionally, the encryption debate was conceptualised as a clash between state security systems and individual privacy rights. However, more recently the debate has been viewed as discourse between those who believe that security is best protected by empowering law enforcement agencies, and those who believe that collective security depends on the integrity of strongly encrypted systems.

There exists a wealth of research assessing the general merits and demerits of providing lawful access to strongly encrypted systems.[[4]](#footnote-4) For example, in his 2015 report, Kaye, then a United Nations Special Rapporteur, argued that restrictions on strong encryption should be limited in order to protect users’ rights to privacy and freedom of opinion and expression online.[[5]](#footnote-5) Baker, former General Counsel at the FBI, has also opposed lawful access, arguing that international cybersecurity threats are so pressing that it is unacceptable to introduce any weakness to encrypted systems.[[6]](#footnote-6) Some further research also exists proposing or evaluating specific lawful access solutions. In 2018, leading figures at GCHQ published their heavily criticised *ghost proposal*, which suggested that government agencies be added to communication channels as silent parties.[[7]](#footnote-7) Lawful hacking has also frequently been advanced as a complete solution.[[8]](#footnote-8) However, even if the lawful access debate can be resolved as it currently stands, as time passes and technology evolves, further debate will be necessitated by new strong encryption technologies. Where once agencies were frustrated by fibre optic cables, now the debate centres on end-to-end and device encryption, and soon quantum computing will change the technological landscape again.[[9]](#footnote-9) As such, in this article we recognise that the encryption debate may never conclusively be resolved, and instead aim to arrive at rules that governments must follow to engage in productive debate and ensure good governance.

The proposed rules arise from an analysis of the lawful access debates in the US and the UK, countries which often work together closely on cybersecurity issues.[[10]](#footnote-10) These jurisdictions have been selected because, as discussed here at 1.3, the debate in each country is at an advanced and pivotal stage. Further, as each country has expressed a wish to influence the encryption debate abroad, it is hoped that recognising the flaws in their discussions will be valuable as other jurisdictions commence or develop their own debates. Part One of this piece provides background on the going dark debate and outlines the key arguments that have been advanced for and against lawful access. In Part Two, it will be shown that continuous open debate must be facilitated in order to prevent the implementation of unsafe lawful access solutions. Finally, in Part Three it will be argued that governments should be held to three rules when engaging in debate about lawful access: legislation governing lawful access must state clearly on its face whether decryption can be mandated; the encryption debate must not be oversimplified or reduced to emotive examples in order to secure public support for unsafe solutions; and safeguards on warrants must not be conflated with safeguards on lawful access mechanisms in order to suggest that solutions are safer than is actually the case.

**1.2: Background on the lawful access debate.**

End-to-end and device encryption are currently the key systems facing regulatory scrutiny in the US and the UK, but friction over lawful access to new technology has been prevalent for decades. McCarthy describes how, faced with new encryption software in the 1990s, the US government attempted to escrow keys under the ultimately commercially unsuccessful Clipper Chip system.[[11]](#footnote-11) Subsequently, when frustrated by the deployment of fibre optic cables, the Communications Assistance for Law Enforcement Act 1994 (CALEA) was implemented, which forced telecommunications carriers to re-engineer their systems to facilitate wiretapping.[[12]](#footnote-12) In the UK, the Government responded to increases in the use of encryption technology by passing the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA facilitated decryption by making it a criminal offence for companies or individuals in possession of encryption keys to fail to hand them to authorities when asked to do so.[[13]](#footnote-13) Over recent years, the lawful access debate in Five Eyes countries[[14]](#footnote-14) such as the US and the UK has centred on end-to-end encryption and device encryption in turn.

End-to-end encryption is newly popular amongst big-tech companies, who seem keen to address privacy concerns amongst their customers following the Snowden revelations.[[15]](#footnote-15) As Kerr and Schnier explain, encryption encodes information by running it through a series of operations dictated by a hidden ‘key’.[[16]](#footnote-16) When end-to-end encryption is used, technology companies do not hold copies of this key, so it is impossible to reverse the operation and decrypt data in transit. As such, law enforcement agencies cannot perform virtual wiretaps on end-to-end encrypted systems. Device encryption differs in that it obscures data at rest, commonly the contents of a phone, which may only be read as plaintext when the user’s password is entered. Apple has used device encryption as standard in their products since 2014.[[17]](#footnote-17) Device encryption became particularly controversial following the San Bernardino and Pensacola terrorist attacks in America, as the FBI were unable to demand that Apple turn over inaccessible data encrypted on the iPhones of each attacker.[[18]](#footnote-18)

Lawful access debates are also ongoing in many other countries. In some jurisdictions, one approach is decisively politically favoured. Both China and Russia regulate encryption extensively and require that technology companies undermine their systems to assist law enforcement agencies.[[19]](#footnote-19) By contrast, the German government has an extensive history of support for strong encryption;[[20]](#footnote-20) law enforcement agencies in Germany may not demand decrypted data, and must instead rely on carefully regulated lawful hacking techniques. A further group of jurisdictions are just beginning to propose tentative legal solutions to the encryption debate. In Australia, the 2018 Assistance and Access Bill[[21]](#footnote-21) granted the Attorney General the heavily criticised power to mandate lawful access.[[22]](#footnote-22) The debates in the US and the UK are at similar crossroads. In a final set of jurisdictions, including Brazil, India, and the EU, the encryption debate remains entirely unresolved in the face of ever-increasing pressure to regulate.[[23]](#footnote-23)

**1.3: Current encryption policy in the US and the UK.**

Although attempts have been made in both the US and the UK to mandate lawful access, the debate is yet fully to be resolved in either jurisdiction. In the UK, the Investigatory Powers Act 2016 (IPA) allows the Secretary of State to impose obligations on telecommunications operators by issuing technical capability notices.[[24]](#footnote-24) The Investigatory Powers (Technical Capability) Regulations 2018[[25]](#footnote-25) have now clarified that the obligation to remove strong encryption may be imposed under the IPA, although Baker notes that it is unclear whether this provision will be effective when used against manufacturers in practice.[[26]](#footnote-26) In March 2019, Mark Zuckerberg published Facebook’s new privacy policy, in which it was announced that end-to-end encryption would be deployed across all Facebook-owned messaging services.[[27]](#footnote-27) Facebook has stated that they cannot implement strong encryption in the immediate future, but their announcement has nevertheless reignited the encryption debate in the US.[[28]](#footnote-28) In July 2019, US Attorney General Barr gave an address in which he argued that lawful access to strongly encrypted communications must be provided in order to prevent serious ‘real world’ harms.[[29]](#footnote-29) The US, UK, and Australian governments have since partnered in opposing unbreakable encryption in open letters and summits.[[30]](#footnote-30) Throughout 2020, multiple attempts have been made in the US to pass legislation mandating lawful access. The EARN IT Bill proposed removing legal content immunity for companies who failed to comply with ‘best practices’.[[31]](#footnote-31) Initially, ‘best practices’ were to be defined by a council overseen by anti-encryption Attorney General Barr,[[32]](#footnote-32) but the Bill has since been amended to limit his influence and protect strong encryption.[[33]](#footnote-33) However, another anti-encryption Bill, the Lawful Access to Encrypted Data Bill, has recently been proposed.[[34]](#footnote-34)

Those currently supporting lawful access in the US and the UK often claim that strong encryption facilitates crime. Technology companies who use strong encryption are unable to process plaintext user data internally, and are therefore unable to report dangerous content to the authorities. In their open letter to Facebook, representatives of the US, UK, and Australian governments noted that Facebook made 16.8 million reports of child exploitation content on their websites in the US in 2018.[[35]](#footnote-35) Facebook reported a further 26 million pieces of terrorist content between October 2017 and March 2019.[[36]](#footnote-36) Since December 2019, the UK’s National Society for the Prevention of Cruelty to Children (‘NSPCC’) has collected over 30,000 signatures on their open letter to Facebook, in which they claim that end-to-end encryption puts children at risk by making it impossible for companies to report dangerous communications.[[37]](#footnote-37) In response, Facebook has claimed that merely assessing the numbers of reports that they make risks overstating the issue, as around 96% of content reports relate to the same pieces of content.[[38]](#footnote-38) Further, it is impossible to know what proportion of reports Facebook makes without conducting plaintext analysis, for example by examining metadata or following a user report, and would therefore still be possible in an end-to-end encrypted system.

Those who oppose lawful access have frequently claimed that crime cannot be prevented by passing legislation to allow law enforcement agencies lawful access to encrypted data. Kerr and Schnier note that no lawful access solution can work consistently, as users will always be able to find alternative software to shield themselves from surveillance.[[39]](#footnote-39) Congresswoman Eshoo and Senator Wyden wrote to Attorney General Barr in 2019, arguing that lawful access legislation would merely encourage criminals to move to unregulated foreign platforms or the dark web,[[40]](#footnote-40) an argument which has since been repeated by Facebook.[[41]](#footnote-41) McCarthy and Pfefferkorn have both argued that criminals can easily use open-source or black market strong encryption products to evade law enforcement,[[42]](#footnote-42) and Ebner recently detailed how extremists already replace platforms which they suspect to be surveilled with ‘alt-tech’ equivalents.[[43]](#footnote-43) It is clearly possible that providing lawful access to the data held by large companies would not stop users from finding ways to encrypt their communications.

Opponents of lawful access have further argued that law enforcement agencies do not genuinely need access to strongly encrypted information. In his UN report, Kaye argued that states have failed to show that strong encryption is a challenge for law enforcement agencies and have actively downplayed the value of alternative investigation techniques.[[44]](#footnote-44) US Government authorities have repeatedly failed to provide data which justifies a need for lawful access; in May 2018, it was reported that the FBI had repeatedly overstated the amount of locked phones that they were unable to access,[[45]](#footnote-45) and it was revealed in December 2019 that the New York District Attorney’s Office had managed to unlock over 60% of phones seized that year, up from around 40% in previous years.[[46]](#footnote-46) Researchers at the R Street Institute have also noted that law enforcement agencies have failed to provide data on how many locked phones are crucial for investigations, as opposed to mere routine seizures.[[47]](#footnote-47) Further, researchers at Harvard’s Berkman Klein Centre have argued that any data deficit caused by end-to-end encryption will be offset by the increasing amount of data that can be harvested from products that cannot be strongly encrypted.[[48]](#footnote-48)

A final set of arguments advanced by critics of lawful access describe the harmful side-effects that may occur should strong encryption be undermined. Firstly, those who oppose lawful access often argue that weakening encryption for domestic law enforcement agencies would inevitably introduce vulnerabilities into strongly encrypted systems, which could then be exploited by criminals or foreign governments. Kaye has argued that it is ‘a seemingly universal position among technologists’ that it is impossible to create a lawful access solution for governments that will not be exploited by hostile actors,[[49]](#footnote-49) a position supported by recent statements from Facebook[[50]](#footnote-50) and the Centre for Democracy and Technology.[[51]](#footnote-51) Further, critics argue that providing lawful access for any one set of countries would set a precedent, allowing countries with very different laws and values to demand equal access to their citizens’ private data.[[52]](#footnote-52) This effect was neatly demonstrated by Attorney General Barr when, during a Lawful Access Summit in October 2019, he justified demanding access to strongly encrypted data by arguing that it was already provided in China and Russia.[[53]](#footnote-53) Critics further argue that mandating lawful access would have negative national economic side-effects, as consumers may choose to purchase strongly encrypted systems over weakened domestic products.[[54]](#footnote-54) Finally, it has been argued that lawful access regulations raise difficult jurisdictional issues, as requests for decrypted data will only be effective if they can be invoked against companies operating overseas.[[55]](#footnote-55) The UK’s IPA 2016 does assert extraterritorial jurisdiction, and this has been criticised by major technology companies, who are concerned that they may become subject to conflicting legislation from multiple jurisdictions.[[56]](#footnote-56) As lawful access proposals have generated such extensive criticism, it is clearly important that ongoing debate be facilitated.

**2: Good encryption policy requires open debate**

**2.1: The dangers of unsafe lawful access.**

Lawful access, or alternatives to it, may be implemented in a number of different ways. Some lawful access alternatives would introduce very little risk to encrypted systems, but other solutions, so called ‘backdoors’, may dangerously weaken strong encryption. We argue here that it is crucial that the implementation of unsafe lawful access solutions be prevented. US Attorney General Barr has argued that it would be desirable to facilitate law enforcement access to strongly encrypted information, even if to do so would involve introducing small weaknesses to cybersecurity systems.[[57]](#footnote-57) However, the introduction of even minor encryption vulnerabilities could bring about serious consequences. Baker argues that cybersecurity amongst the US and its allies is ‘woefully subpar’ in the face of sophisticated malicious attacks orchestrated by organised crime and terror groups and hostile nation-states.[[58]](#footnote-58) Further, representatives from Apple have claimed that cyberattacks are increasingly prevalent and sophisticated, an effect that will only increase as more devices are added to the internet.[[59]](#footnote-59) Critics have noted that important and sensitive data relating to health, politics, economics, and the communications of religious groups and dissidents are likely to be targeted by hostile actors.[[60]](#footnote-60)

Introducing vulnerabilities into strongly encrypted systems also risks seriously endangering members of vulnerable or minority groups, and may compromise official communications. The Carnegie Endowment Group argue that strong encryption protects ‘journalists, activists, and marginalized groups’ from surveillance which could lead to persecution.[[61]](#footnote-61) In his UN report, Kaye listed numerous vulnerable groups, including political and religious minorities, researchers, journalists, and lawyers for whom secure encryption offers necessary protection from hostile states.[[62]](#footnote-62) Zuckerberg claims to have spoken to dissidents who have had their lives or liberties saved by the use of strong encryption.[[63]](#footnote-63) Attorney General Barr has claimed that when ‘consumer products’ are discussed ‘we are not talking about protecting the Nation’s nuclear launch codes’, and therefore end-to-end encryption offers superfluous protection.[[64]](#footnote-64) However, *consumer products* are not only used to protect the physical safety of persecuted groups, but also to protect internal government communications. As Schneier points out, there is no longer any difference between many of the technological products used by governments and consumers.[[65]](#footnote-65) Congresswoman Eshoo and Senator Wyden state that Signal and WhatsApp are used for internal communications inside the US Government,[[66]](#footnote-66) and Facebook have claimed that the Senate uses Telegram to communicate.[[67]](#footnote-67) As the US Government use end-to-end encrypted consumer technology internally, any risk introduced to these systems may undermine official communications.

The exploitation of previous lawful access systems show that serious harm is likely to occur should an unsafe lawful access solution be implemented again. As discussed here at 1.2, CALEA 1994 mandated lawful access to telephone communications in the US.[[68]](#footnote-68) In 2011, a former technical director of the US National Security Agency’s (‘NSA’) Information Assurance Division revealed that there were security problems with CALEA implementation on every switch submitted for testing.[[69]](#footnote-69) One of the most serious security issues caused by a lawful access system was the ‘Athens Affair’, during which Vodafone’s lawful access system, modelled on CALEA-compliant switches from the US, was exploited to intercept the communications of the Greek Prime Minister and some one hundred other officials.[[70]](#footnote-70) It has since been revealed that the body responsible for exploiting lawful access in the Athens Affair was the NSA themselves, which the Snowden documents reveal, commonly targets lawful access mechanisms to spy on foreign states.[[71]](#footnote-71) A further example of the malicious exploit of lawful access involves Microsoft’s Golden Key internal backdoor, which was discovered in 2016 and could have enabled the development of malicious versions of Windows.[[72]](#footnote-72) Further, the NSA’s EternalBlue hacking tool was exploited by foreign state hackers in 2019,[[73]](#footnote-73) and it has just been reported that Huawei can access mobile networks around the world via lawful access mechanisms.[[74]](#footnote-74) Squires, speaking on behalf of the UK Government, has claimed that technology companies should be able to protect user data sufficiently without using unbreakable encryption, but large companies and governments have repeatedly failed to mitigate the risk created by lawful access systems.[[75]](#footnote-75) Despite being proposed by national cybersecurity experts, GCHQ’s recent ‘ghost’ proposal for lawful access was dismantled by civil society organisations, academics, and technology companies within six months.[[76]](#footnote-76)

**2.2: Recent progress due to open debate on lawful access.**

Over the last few years, parties on all sides of the encryption debate have recognised that open multidisciplinary debate is necessary in order to find safe lawful access solutions. The R Street Institute stated in their 2018 report that, as adversarial testing is needed in order to ensure that lawful access mechanisms are secure, a safe solution will only be found if open debate is facilitated.[[77]](#footnote-77) In GCHQ’s ghost proposal, Levy and Robinson encouraged honest discussion between experts in order to evaluate proposals,[[78]](#footnote-78) and in 2019 the Five Eyes government partnership called for ‘detailed engagement’ between technology companies, governments, and other relevant parties.[[79]](#footnote-79) As recently as December 2019, Squires stated that the UK Government recognised that ‘ongoing, open and transparent dialogue’ must be facilitated in order to identify safe lawful access solutions.[[80]](#footnote-80) Recent progress in the encryption debate is a direct result of this cross-disciplinary support for transparent debate. In July 2019, US Attorney General Barr acknowledged that, through open debate, promising lawful access solutions were beginning to emerge,[[81]](#footnote-81) a position supported by the Director of the FBI the following October.[[82]](#footnote-82)

One proposal that has been evaluated whilst open debate has been encouraged is the use of metadata, or data which describes communications, in place of plaintext content data. Analysing metadata does not reveal the content of messages, but does reveal information about the location that messages were sent from, timing and rates of communication between parties, and can uniquely identify suspects and accomplices.[[83]](#footnote-83) The usefulness of metadata has repeatedly been contested by law enforcement agencies, with the Director of the FBI dismissing it as ‘timestamps and address blocks.’[[84]](#footnote-84) Government officials in the US and the UK have stated that, as metadata cannot reveal information about a suspect’s mind-set or specific plans, it is of limited use in investigations.[[85]](#footnote-85) When asked about the usefulness of metadata at a summit in October 2019, UK Home Secretary Patel thought it appropriate to scoff on stage.[[86]](#footnote-86) However, Baker has stated that, whilst his experience at the FBI has led him to recognise that metadata is not as useful as plaintext content data, he believes that it can be of use in conjunction with artificial intelligence techniques.[[87]](#footnote-87) Zuckerberg has stated that Facebook is currently developing machine learning tools that will analyse metadata in order to identify suspicious patterns of communication.[[88]](#footnote-88) As Baker has recognised, whilst metadata may not be immediately as useful as content data when surveilling systems, the sheer quantity of metadata stored by companies means that it should be of some use if analysed using artificial intelligence.[[89]](#footnote-89)

A further alternative to lawful access recently analysed through interdisciplinary debate is the use of plaintext copies of, or alternatives to, strongly encrypted data. Kerr and Schneir argue that the identification of an unencrypted copy of user data is often a viable encryption workaround.[[90]](#footnote-90) Most data stored on the cloud is currently not strongly encrypted, as companies hold keys to this data in order to recover lost accounts for their clients.[[91]](#footnote-91) Vance, District Attorney for New York County, has argued that cloud copies are not as useful as direct access to strongly encrypted data, as many users choose not to back up all of their communications.[[92]](#footnote-92) However, researchers at the Carnegie Endowment Group and the Berkman Klein Centre have argued that a further wealth of data remains available to law enforcement agencies via apps that cannot support strong encryption. It is unlikely that companies will choose to strongly encrypt user data where it is profitable for them to analyse that data, for example to target advertisements, or where the functionality of a product depends on access to that data, for example where powerful central processors must be used.[[93]](#footnote-93) As such, it has been proposed that access to data that cannot be strongly encrypted on clouds or alternative apps can provide sufficient lawful access to tackle online crime.

Lawful hacking is another complete solution to the lawful access debate that has been debated recently.[[94]](#footnote-94) Kerr and Schnier describe how authorities can surveil suspects by finding copies of encryption keys, guessing keys, exploiting weaknesses in encryption schemes, or accessing data once it has been decrypted on a device.[[95]](#footnote-95) Tait has argued that wiretapping via lawful hacking is an attractive and proportionate tool, a statement which seems supported by the success of recent law enforcement investigations.[[96]](#footnote-96) Following both the San Bernardino and Pensacola attacks, the FBI were able to bypass Apple’s device encryption by employing lawful hacking techniques.[[97]](#footnote-97) In Germany, where lawful hacking is regulated and supported by the government, the Federal Office for Criminal Investigation successfully hacked Telegram in 2014, unlocking the full message history of eight suspects.[[98]](#footnote-98) However, parties on all sides of the encryption debate have noted flaws with lawful hacking. Vance notes that the purchase or development of lawful hacking software is often prohibited by cost, especially amongst smaller law enforcement agencies.[[99]](#footnote-99) Further, lawful hacking can undermine national cybersecurity by creating a marketplace for exploits, revealing data in excess of what is required for investigations, and disincentivising the disclosure of security vulnerabilities to technology companies.[[100]](#footnote-100) Liguori argues that many of the issues caused by lawful hacking could be fixed by developing robust regulation,[[101]](#footnote-101) but laws in this area currently remain severely underdeveloped.[[102]](#footnote-102)

A final set of solutions that have been explored whilst open debate has been encouraged include on-device key escrow, wider exchange of information about data, and the implementation of proactive safety solutions. Firstly, both the R Street Institute and the Carnegie Endowment Group have proposed that lawful access could be facilitated for data at rest through on-device key escrow.[[103]](#footnote-103) On-device escrow would allow law enforcement agencies with physical access to a strongly encrypted device to access encrypted data once a set safety procedure has been followed. Secondly, the wider exchange of information about data may allow technology companies and law enforcement agencies to work together to better utilise data that is already available. When asked what solutions short of lawful access could aid law enforcement agencies, Vance responded that clear communication about what data is held by technology companies would be helpful.[[104]](#footnote-104) Similarly, it has been proposed that law enforcement agencies should release clearer information on what user data they need in order to allow technology companies to develop useful tools.[[105]](#footnote-105) Finally, proactive safety solutions, such as those currently being developed by Facebook, could reduce the need for lawful access by preventing crime from occurring in the first place. Facebook have stated that they aim to use artificial intelligence to prevent crime on their platforms, and in May 2020 they announced the release of safety notices on Messenger which encourage users to self-report suspicious communications.[[106]](#footnote-106) No one proposal has solved the lawful access debate as it stands, but some combination of the techniques described in this section would undeniably help law enforcement agencies to combat crime in the face of new strong encryption technologies. It would appear from these examples that open and transparent discourse has allowed progress to be made in the lawful access debate.

**2.3: Increasing governmental pressure to find a lawful access solution.**

It is our view that open debate over lawful access will continue to be necessitated by the evolution of technology, and as such governments must not prematurely close discussions by imposing reactive legislation. The worst case scenario in the lawful access debate is that governments attempt to impose permanent unsafe solutions in response to a terrorist or other emergency attack, a situation that is agreed to be increasingly likely.[[107]](#footnote-107) GCHQ have acknowledged that investigative tradecraft must continue to evolve as new technology is developed, as solutions proposed now will cease to be effective when companies deploy new systems.[[108]](#footnote-108) The Carnegie Endowment Group have argued that quantum computers capable of threatening current encryption techniques may be available within the next ten to twenty years.[[109]](#footnote-109) Therefore, even if a safe way to implement lawful access in our current technological landscape can be identified, the techniques used may be rendered unsafe by novel technologies such as quantum computing very quickly. As Rozenshtein has argued, the encryption debate is so complex and liable to change that no one solution will ever permanently end it.[[110]](#footnote-110) As such, states must commit to ongoing collaboration rather than threatening artificially to curtail discussions.

Recently, the governments in the US and the UK have increasingly exerted time pressure on the lawful access debate, which risks forcing the implementation of a dangerous lawful access solution. In June 2020, the Five Eyes government partnership stated that ‘technology companies need to work quickly’ to solve the debate.[[111]](#footnote-111) In the UK, Home Secretary Patel released a statement in July 2019 which suggested that immediate action should be taken to combat strong encryption.[[112]](#footnote-112) Patel’s actions are especially threatening in light of Section 255(8) of the IPA 2016, which renders it illegal for a person forced to remove strong encryption by the UK Government to reveal this to anybody else without the permission of the Secretary of State.[[113]](#footnote-113) If the UK Government wished to shut down the lawful access debate and enforce an unsafe solution, they could arguably do so without there being any possibility of the public becoming aware that encryption had been dangerously undermined.

In the US, Attorney General Barr has also repeatedly pressured the lawful access debate, stating that time is limited in which the government will remain ‘open to a cooperative approach.’[[114]](#footnote-114) In December 2019, Lindsey Graham, Chair of the Senate Judiciary Committee, threatened to force through a legislative solution if technology companies could not facilitate lawful access to strongly encrypted information quickly.[[115]](#footnote-115) Since then, Graham has proposed two Bills designed to undermine encryption. The EARN IT Bill proposed removing the protection provided by s230 of the Communications Decency Act 1996 (CDA) from companies that did not follow ‘best practices’, which could have included the removal of strong encryption.[[116]](#footnote-116) Following amendments to EARN IT which protected encryption,[[117]](#footnote-117) Graham proposed the Lawful Access to Encrypted Data Bill. Where EARN IT only covertly affected strong encryption, Graham’s new Bill has been described as a blatant and sweeping attempt to demand access.[[118]](#footnote-118) There is an increasing chance that an unsafe lawful access solution will be mandated in the US in the very near future. Ongoing and transparent debate is, we believe, the best way to ensure that this does not happen.

**3: Three rules to facilitate the lawful access debate**

**3.1: The value of international rules.**

The governments in the US and the UK seem increasingly determined to impose unsafe lawful access solutions that risk compromising the integrity of strongly encrypted systems. Analysis of lawful access debates in the US and the UK suggests that governments have undermined the debate in three key ways. Firstly, deliberately ambiguous legislation has been proposed in order to avoid public scrutiny; once this legislation has been enacted, powers have been used expansively in order to mandate unsafe lawful access solutions. Secondly, governments have oversimplified the encryption debate and relied on emotive examples in order to garner public support for unsafe solutions. Finally, officials have falsely implied that, where warrants are subject to appropriate legal safeguards, lawful access solutions must also be safe. The deliberate conflation of safeguards on warrants with safeguards on lawful access mechanisms has risked lending false legitimacy to unsafe solutions. It is proposed that governments should avoid these three practices in order to facilitate the ongoing debate necessary to find safe lawful access solutions.

Lawful access solutions inevitably involve international cooperation, and jurisdictions are likely to attempt to influence encryption policy abroad. The EastWest Institute have argued that, due to the global nature of technology, lawful access solutions will only be effective if they are supported internationally.[[119]](#footnote-119) The Carnegie Group agree, noting that the burden of implementation on technology companies will be too great if international solutions cannot be found.[[120]](#footnote-120) The rules suggested in this paper would support international dialogue by upholding common minimum standards in the lawful access debate. Further, representatives of both the US and UK governments have suggested that their own lawful access debates should influence policy overseas. In July 2019, US Attorney General Barr suggested that American companies should ‘advance their interests’ by influencing encryption policy worldwide.[[121]](#footnote-121) The following October, UK Home Secretary Patel stated that the UK must ‘lead the world’ in the lawful access debate.[[122]](#footnote-122) As the US and UK seem intent on influencing policy abroad, it is clearly important to learn from the flaws in their national debates.

**3.2: Rule One: Decryption powers should be clear on the face of legislation.**

The lawful access debate has been compromised in both the US and the UK by the use of ambiguous legislation which has had limited public scrutiny. In the UK, the ambiguity of the IPA 2016 undermined the lawful access debate by compromising discussions in Parliament.[[123]](#footnote-123) The full extent of the powers granted under the IPA are only now fully being acknowledged by the Government, three years after the Act came into force. In the US, the proposed EARN IT Bill could have seriously undermined the encryption debate in early 2020.[[124]](#footnote-124) By disguising the EARN IT as a change to s230 of the CDA 1996, a publicly unpopular legal provision, legislators threatened to mandate decryption without attracting necessary public attention.[[125]](#footnote-125) Governments engaging in lawful access debates must ensure that any legislation proposed states clearly on its face whether it may be used to force companies to alter strongly encrypted systems.

Speaking on behalf of the UK Government, Squires has argued that the IPA 2016 provides a ‘clear legal framework’ on encryption.[[126]](#footnote-126) Squires justifies her claim by relying on the fact that the Act was analysed in multiple reports, committees, and debates prior to its implementation.[[127]](#footnote-127) However, as the powers granted under the IPA would appear to have been somewhat obscured during its journey through Parliament, the Act was passed without full debate on lawful access ever taking place in the UK. The IPA allowed the Home Secretary to impose certain ‘obligations’ on technology companies, but the Act did not state whether the obligation to remove strong encryption could be imposed.[[128]](#footnote-128) When questioned on the extent of the obligations that may be imposed under the Act during debates, the Government repeatedly stated that the Home Secretary could not ask technology companies to take steps that were not ‘reasonably practicable’. Reasonable practicability has been described as a ‘key legal test’ by Squires, despite the term being inherently ambiguous.[[129]](#footnote-129) When defending the Bill in the House of Lords, Earl Howe frequently evaded questions about whether the IPA could be used to mandate decryption by relying on the concept of reasonable practicability.[[130]](#footnote-130) Crucially, Lord Harris argued during debates that, as it was not possible to know how future Home Secretaries would interpret reasonable practicability, it was impossible to understand how the IPA would affect strongly encrypted systems.[[131]](#footnote-131) As such, when the IPA was enacted in the UK, it was unclear whether lawful access could be mandated under the Act.

The ambiguity in the IPA 2016 has further undermined open debate by allowing the Government gradually to expand the powers granted under the Act in order to demand lawful access. During Parliamentary debates, Lord Strasburger questioned why, if the IPA could not be used as a legal basis for lawful access, this should not be included on the face of the Act.[[132]](#footnote-132) The IPA was described as ‘opaque’ in written evidence provided by prominent technology companies, who also questioned why, if the Act was not intended to weaken strong encryption, this was not expressly stated.[[133]](#footnote-133) Some clue as to the purpose of the ambiguity in the IPA can be gleaned from the comments of the Solicitor General, who suggested that the Act should be clarified in its Code of Practice, a ‘flexible, living instrument’ capable of keeping pace with technology.[[134]](#footnote-134) This comment suggests that the ambiguity in the IPA was a conscious governmental choice, despite it undermining the lawful access debate in Parliament. In regulations published in 2018, it was clarified that the obligation to remove encryption can be imposed under the IPA.[[135]](#footnote-135) In December 2019, Squires finally publicly acknowledged that the IPA can provide a legal basis for lawful access requests.[[136]](#footnote-136) By slowly ‘clarifying’ the Act over three years, rather than debating its provisions openly at the outset, the Government in the UK has, in our view, failed properly to engage in the lawful access debate, and has granted itself the power unilaterally to mandate an unsafe lawful access solution.

In the US, the proposed EARN IT legislation risked undermining the encryption debate by burying lawful access powers in a Bill that appeared to relate to an entirely separate legal issue.[[137]](#footnote-137) Section 230 of the CDA 1996 grants technology companies legal immunity for public content posted by users of their sites.[[138]](#footnote-138) Section 230 is increasingly controversial in the US, as the public have begun to resent the role of large technology companies in surveilling customers and spreading harmful or false content.[[139]](#footnote-139) The EARN IT Bill would have removed providers’ controversial s230 immunity if they failed to comply with ‘best practices’, which could have included an obligation to remove strong encryption.[[140]](#footnote-140) As such, Pfefferkorn argues that the EARN IT Bill was a ‘bait and switch’, in which the anti-encryption proponents of the Bill capitalised on resentment for s230 in order covertly to undermine strong encryption.[[141]](#footnote-141) Strong encryption is currently protected in the US under CALEA 1994[[142]](#footnote-142) which expressly distinguishes strong encryption from wiretapping and prevents mandated decryption being implemented in this area.[[143]](#footnote-143) As Pfefferkorn argues, if legislators wish to mandate lawful access, this can only properly be done by debating amendments to CALEA.[[144]](#footnote-144) Where Governments attempt to regulate lawful access by passing ambiguous or covert legislation, they deliberately limit the encryption debate and risk forcing through unsafe solutions that could place users of strongly encrypted services in danger.

**3.3: Rule 2: The lawful access debate should not be deliberately oversimplified and emotive examples should not be used to influence public opinion.**

Government officials in both the US and the UK have, in our view, compromised the encryption debate by attempting to garner public support for unsafe lawful access solutions. Governments have sought to influence the public in two key ways. Firstly, officials have oversimplified the encryption debate by focussing exclusively on how enhanced surveillance powers may help to prevent crime. By focussing on the prevention of especially shocking crimes, and by failing to acknowledge that the implementation of lawful access may be dangerous in itself, governments have artificially increased public support for unsafe solutions.[[145]](#footnote-145) Secondly, officials have frequently relied upon appalling and emotive examples of online crime in order to generate distrust of strong encryption technology.[[146]](#footnote-146) The public are liable to be influenced by the use of shocking and emotive examples. Law enforcement agencies in the US have acknowledged that, in light of recent scandals such as the Cambridge Analytica affair, public support for technology companies is waning.[[147]](#footnote-147) Attorney General Barr has gone as far as to suggest that ‘it is only a matter of time before a sensational case crystallises the issue for the public.’[[148]](#footnote-148) In our view, where governments attempt to influence the public by oversimplifying the encryption debate or relying on emotive examples, this risks undermining open debate, increasing the likelihood that a dangerous solution will be imposed.

The governments in the US and the UK have frequently argued that they must be provided with lawful access to strongly encrypted data in order to combat serious crimes such as terrorism, violent offences, and child abuse.[[149]](#footnote-149) Officials have claimed that strongly encrypted systems are exploited by criminals, who find it increasingly easy to make plans and share illegal content online. However, representatives from government, academia, and law enforcement have all argued that recent focus on the prevention of serious crime is merely a strategy used by governments to justify undermining strongly encrypted systems.[[150]](#footnote-150) In October 2019, Congresswoman Eshoo and Senator Wyden argued that, as the US Government was failing to take less intrusive steps to tackle online crime, the protection of children was merely a ‘false pretense’ being used to weaken encryption.[[151]](#footnote-151) This claim seems persuasive; as of September 2019 the US Justice Department had failed to produce four of the six reports that it was legally required to make relating to crimes against children[[152]](#footnote-152) and a former FBI employee has argued that increases in crimes against children represent failures that are more complex and systemic than the uptake of strong encryption.[[153]](#footnote-153) Finally, Pfefferkorn has noted that the EARN IT Bill, which was premised on protecting children online, would not have created any legal tools that were not already available to law enforcement agencies.[[154]](#footnote-154) Whilst it is clearly enormously important to tackle serious online crime, this must be done safely, by funding law enforcement agencies properly and making full use of existing legal powers. The fact that horrible crime exists online should not be used to justify mandating lawful access in a way that risks causing other types of serious harm, such as the persecution of vulnerable groups or the theft of personal data.

Examples of the use of oversimplified narratives and reliance on emotive examples have been prevalent recently in both the US and the UK. In July 2019, Attorney General Barr attempted to generate distrust of strongly encrypted systems by linking them to the murder of police officers by a Mexican cartel, two ISIS attacks, human trafficking, and paedophilia.[[155]](#footnote-155) In the same month, Home Secretary Patel implied that lawful access could have prevented the Christchurch shooting, foreign disinformation campaigns, and increases in child exploitation, despite making no attempt to link these offences to strong encryption technology.[[156]](#footnote-156) The Five Eyes group cited nonspecific concerns about strong encryption being used to undermine democratic values in their 2019 inter-governmental report, but failed to mention the security benefits of encryption technology.[[157]](#footnote-157) Government officials have repeatedly attempted to justify lawful access by explaining specific criminal acts in graphic detail.[[158]](#footnote-158) Further, the UK NSPCC’s open letter bears striking resemblance to the open letter sent to Facebook by the US, UK, and Australian governments, showing that oversimplified narratives advanced by governments are gaining traction in public discourse.[[159]](#footnote-159) In October 2019, the US Government held a summit on lawful access at which technology companies were refused a platform in order to focus on ‘the human cost of technology.’[[160]](#footnote-160) The summit involved emotional accounts being given by the victims of crime and representative organisations. Discussing how to prevent online crime is of vital importance, but failing to invite technology companies to the table risks the implementation of disproportionate solutions which may cause further harm. Discussions about the benefits and disbenefits of lawful access must be balanced and truly interdisciplinary, in order to prevent the implementation of impulsive and dangerous policies.

A final example of the uptake of oversimplified government narratives on strong encryption relates to the increasing use of specific language relating to *safe spaces* being provided for criminals. Shortly after the 2015 Paris terrorist attacks, UK Prime Minister David Cameron stated that strong encryption must not provide criminals with a ‘safe space’ on the internet.[[161]](#footnote-161) Since this statement, similar language has been used widely by governments to discredit strong encryption technologies. Barr has added hyperbole to the discussion by referencing the ‘impenetrable cloak of secrecy’ and ‘law-free zones’ that he believes are facilitated by strong encryption technologies.[[162]](#footnote-162) Similarly, the Director of the FBI has referenced ‘lawless space[s]’,[[163]](#footnote-163) Patel has discussed ‘spaces for criminality’,[[164]](#footnote-164) and Senator Graham has used the term ‘a safe haven for criminality.’[[165]](#footnote-165) These linguistic tropes, advanced by government officials, have since taken root in public discourse. The New York Times have referenced ‘hiding places’ being provided for criminals,[[166]](#footnote-166) and the NSPCC have repeatedly stated that strong encryption offers criminals ‘a place to hide’ online.[[167]](#footnote-167) Clearly, the oversimplified narratives that have been propagated by the US and UK Governments are gaining traction in wider civil society.

It seems to us irresponsible that governments should garner public support for dangerous solutions by relying on oversimplified narratives, as this risks compromising legislative debates. The support generated for these narratives has already enabled defenders of legislation in the US and the UK to attempt to justify decryption powers by relying on emotive examples. In UK IPA debates, the Solicitor General defended mandated decryption by citing concerns over terrorists and paedophiles.[[168]](#footnote-168) In the US, congressional findings in the Lawful Access to Encrypted Data Bill state that decryption is necessary to prevent child abuse, terrorism, and international narcotics trafficking.[[169]](#footnote-169) The US Bill also advances the ‘safe spaces’ linguistic trope analysed previously by stating that strong encryption enables a ‘lawless space’.[[170]](#footnote-170) As such, we argue that governments should not promote oversimplified or emotive narratives, as to do so may facilitate the enactment of unsafe lawful access solutions

**3.4: Rule Three: Safeguards applicable to warrants should not be conflated with safeguards applicable to lawful access mechanisms.**

A final way that governments have undermined the lawful access debate in the US and the UK, is by deliberately conflating safeguards on warrants with safeguards on lawful access mechanisms. In order to access user data for use in an investigation, law enforcement agencies must satisfy two criteria. Firstly, certain legal requirements must be met in order for an agency to be granted a warrant, which they may then serve on a technology company in order to request relevant data.[[171]](#footnote-171) Secondly, it must be technologically possible for the technology company in question to provide the data requested.[[172]](#footnote-172) This article has discussed the second of these stages, as where strong encryption technology is employed, it is impossible for companies to hand over useable data in plaintext format. However, Government officials in the US and the UK have repeatedly conflated this second stage with the issue of the acquisition of warrants, in order to suggest that implementing lawful access would be safer than is actually the case. The argument is as follows: if law enforcement agencies have complied with all of the safeguards required for a warrant to be granted, surely it is then safe to require that this data is actually handed over in a readable format. However, when governments conflate warrant safeguards with lawful access safeguards, they fail to recognise that facilitating lawful access creates vulnerabilities in systems *before* warrants are even requested; in our view this fallacy undermines the encryption debate.

The UK Government have repeatedly conflated warrant safeguards and lawful access safeguards when discussing the IPA 2016.[[173]](#footnote-173) When the IPA was debated in May 2016, the Solicitor General stated that lawful access mechanisms need not be subject to extensive legal protections, as they were merely ‘preliminary steps’ designed to secure subsequent compliance with warrants.[[174]](#footnote-174) However, as Apple, Facebook, Google, Microsoft, Twitter, and Yahoo have pointed out, cybersecurity may be damaged as soon as companies are forced to implement unsafe lawful access solutions, as systems may be exploited from this point onwards.[[175]](#footnote-175) As such, the safeguards applicable to warrants are entirely irrelevant to the lawful access debate. In December 2019, Squires suggested that lawful access was safe in the UK because only targeted data could be requested, and only by specific bodies where to do so was necessary and proportionate.[[176]](#footnote-176) By listing these protections, Squires would appear to have lent a false legitimacy to lawful access legislation. Regardless of whether warrants are served on companies in safe ways, the very existence of lawful access mechanisms can create dangerous vulnerabilities in systems. As such, the safeguards applicable to warrants must not be used to suggest that it is safe to undermine strongly encrypted systems.

Since the IPA debates, conflation of safeguards has also begun to take place in the US. Recently, Attorney General Barr has described strong encryption as ‘warrant proof’, a term designed to encourage this very type of conflation.[[177]](#footnote-177) By using the term ‘warrant proof’, Barr deliberately minimises the role that strong encryption plays in protecting cybersecurity, suggesting instead that the technology merely exists to frustrate law enforcement agencies.

Safeguard conflation has also been used in the US to disincentivise use of the term ‘backdoor’, which the government oppose. Vance, District Attorney for New York County, has suggested that lawful access mechanisms are not equivalent to ‘backdoors’ into encrypted systems, as they will only be used following approval from impartial judges.[[178]](#footnote-178) Whether there is any rational distinction between encryption backdoors and lawful access mechanisms will depend on the specific details of their implementation, but this distinction certainly cannot be justified by reference to irrelevant safeguards on warrants. Further, US officials have recently begun to refer to lawful access solutions as ‘front doors’, implying that, as lawful access will only be utilised when warrants have been granted, it must be safe to bypass strong encryption.[[179]](#footnote-179) By referencing the impartiality of judges issuing warrants and focussing on the limited categories of data that may be collected, governments have encouraged the public to believe that lawful access mechanisms will be safe, without discussing the fact that they may be exploited by malicious actors before any warrant is ever even considered. Governments should not conflate the safeguards applicable to warrants with the safeguards applicable to lawful access solutions, as to do so compromises the encryption debate by suggesting that lawful access solutions are safer than is actually the case.

**3.5: Conclusion.**

Safe lawful access solutions will only be identified if transparent debate is facilitated. As technology evolves, lawful access solutions will inevitably also need to be updated, and as such the lawful access debate will not ever permanently be resolved. It has been proposed that, in order to facilitate the ongoing and transparent debate necessary to prevent the implementation of unsafe lawful access solutions, governments should follow three rules:

1. Any proposed legislation should state clearly on its face whether it can be used to mandate lawful access to strongly encrypted systems. Adherence to this rule will prevent governments from unsafely bypassing the encryption debate by enacting ambiguous or covert decryption powers, as was the case when the IPA 2016 and the EARN IT Bill were proposed.
2. Government officials should not deliberately oversimplify the encryption debate or rely on emotive examples in order to influence public opinion. Adherence to this rule will ensure that governments cannot garner public support for dangerous lawful access solutions which risk compromising secure systems.
3. The safeguards applicable to warrants must not be conflated with the safeguards applicable to lawful access solutions in order to lend false legitimacy to unsafe solutions. Adherence to this rule will prevent governments from compromising open debate by suggesting that warrant safeguards have made it safe to undermine strongly encrypted systems.

These rules are proposed in the hope that they may influence the ongoing lawful access debates within the US and the UK. As the debates are now reaching pivotal moments in each jurisdiction, it is important that governments continue to be held to standards which reduce the likelihood that unsafe solutions will be imposed. Further, it is hoped that the suggestions in this paper may be used to evaluate encryption debates in other jurisdictions, especially where the debate remains at a more preliminary stage. The US and the UK have expressed a desire to influence encryption policy beyond their jurisdictions, and as such it is vital that we learn from the mistakes in their lawful access debates in order to protect global cybersecurity.

**Reference List**

Regulation of Investigatory Powers Act 2000 pt III (United Kingdom).

Investigatory Powers Act s 253 and 255 (United Kingdom).

Investigatory Powers (Technical Capability) Regulations 2018 (United Kingdom).

Communications Assistance for Law Enforcement Act 1994 (United States).

Communications Decency Act 1996 s 230 (United States).

US Senate 116th Congress *S 3398 Eliminating Abusive and Rampant Neglect of Interactive Technologies Act* (Washington: Government Printing Office 2020) (United States).

US Senate 116th Congress *S 4051 Lawful Access to Encrypted Data Act* (Washington: Government Printing Office 2020) (United States).

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Australia).

-- Carnegie Encryption Working Group, ‘Moving the Encryption Policy Conversation Forward’ (Carnegie Endowment for International Peace 2019) <https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573> accessed 3 September 2020.

-- Five Eyes Country Ministerial communiques, ‘Joint meeting of Five Country Ministerial and quintet of Attorneys-General: communique, London 2019’ (UK Government 2019) <https://www.gov.uk/government/publications/five-country-ministerial-communique> accessed 3 September 2020.

-- HC Deb 3 May 2016, vol 609, col 645 at <https://bit.ly/3i1RjC8>.

-- HL Deb 13 July 2016, vol 774 at <https://bit.ly/2Dr8ldQ>; <https://bit.ly/351KPiS>; <https://bit.ly/2QYG9C5>.

-- HL Deb 19 October 2016, vol 774 at <https://bit.ly/2ZPxAME>.

-- ‘Home Secretary chairs virtual ‘Five Eyes’ security summit’ (UK Government 2020) <https://www.gov.uk/government/news/home-secretary-chairs-virtual-five-eyes-security-summit> accessed 3 September 2020.

-- The Guardian, *‘The NSA Files’* (The Guardian) <https://www.theguardian.com/us-news/the-nsa-files> accessed 3 September 2020.

-- Joint Committee on the Draft Investigatory Powers Bill, ‘Volume of Written Evidence’ (UK Parliament 2016) <https://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-investigatory-powers-bill/publications/> accessed 3 September 2020.

-- National Society for the Prevention of Cruelty to Children, ‘Our letter to Facebook’ (National Society for the Prevention of Cruelty to Children 2019) <https://www.nspcc.org.uk/about-us/news-opinion/2019/facebook-encryption-sexual-abuse/> accessed 3 September 2020.

-- Princeton University Centre For Information Technology Policy and Carnegie Endowment for International Peace, ‘Likely Future Adoption of User-Controlled Encryption’ (Carnegie Endowment 2019) <https://carnegieendowment.org/2019/04/25/likely-future-adoption-of-user-controlled-encryption-pub-78986> accessed 3 September 2020.

-- Princeton University Centre For Information Technology Policy and Carnegie Endowment for International Peace, ‘Implications of Quantum Computing for Encryption Policy’ (Carnegie Endowment 2019) <https://carnegieendowment.org/2019/04/25/implications-of-quantum-computing-for-encryption-policy-pub-78985> accessed 3 September 2020.

-- Privacy International, ‘Five Eyes’ (Privacy International) <https://privacyinternational.org/learn/five-eyes> accessed 3 September 2020.

-- UK Parliament, ‘Investigatory Powers Bill: Written Evidence submitted by Apple Inc, Facebook Inc, Google Inc, Microsoft Corp, Twitter Inc and Yahoo Inc’ (UK Parliament 2016) <https://publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB21.htm> accessed 3 September 2020.

Aleixo G, Guimaraes Gobbato A, Garcia De Souza I, Langenegger N, Lemos R and Steibel F, ‘The Encryption Debate in Brazil’ (Carnegie Endowment for International Peace 2019) <https://carnegieendowment.org/2019/05/30/encryption-debate-in-brazil-pub-79219> accessed 3 September 2020

Baker J, ‘Rethinking Encryption’ (Lawfare 2019) <https://www.lawfareblog.com/rethinking-encryption> accessed 3 September 2020.

Barr W, ‘Keynote Address’ (International Conference on Cyber Security at Fordham University 2019) <https://www.lawfareblog.com/attorney-general-delivers-address-encryption-cybersecurity-conference> accessed 3 September 2020.

Barr W, ‘Remarks as Prepared for Delivery at Lawful Access Summit’ (US Department of Justice 2019) <https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-lawful-access-summit> accessed 3 September 2020.

Bedell Z and Major J, ‘What’s Next for Section 230? A Roundup of Proposals’ (Lawfare 2020) <https://www.lawfareblog.com/whats-next-section-230-roundup-proposals> accessed 3 September 2020.

Bradford Franklin S and Wilson Thompson A, ‘Open Letter to GCHQ on the Threats Posed by the Ghost Proposal’ (Lawfare 2019) <https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal> accessed 3 September 2020.

Brewster T, ‘FBI Hacks iPhones In Pensacola Terrorist Shooting Case, But the War With Apple Goes On’ (Forbes 18 May 2020) <https://www.forbes.com/sites/thomasbrewster/2020/05/18/feds-hack-iphones-in-pensacola-case-apple-not-needed-after-all/#9491dcb75e99> accessed 3 September 2020.

Cathcart W and Chudnovsky S, ‘Facebook’s Public Response to Open Letter on Private Messaging’ (Facebook 2019) <https://about.fb.com/news/2019/12/facebooks-response-to-open-letter-on-private-messaging/> accessed 3 September 2020.

Cook T, ‘A Message to Our Customers’ (Apple 2016) <https://www.apple.com/customer-letter/> accessed 3 September 2020.

Crocker A, ‘The Senate’s New Anti-Encryption Bill Is Even Worse Than EARN IT, and That’s Saying Something’ (Electronic Frontier Foundation 2020) <https://www.eff.org/deeplinks/2020/06/senates-new-anti-encryption-bill-even-worse-earn-it-and-thats-saying-something> accessed 3 September 2020.

Duan C, Rizer A, Graves Z and Godwin M, ‘Policy Approaches to the Encryption Debate’ (R Street Institute 2018) 5 <https://www.rstreet.org/2018/03/05/policy-approaches-to-the-encryption-debate/> accessed 3 September 2020.

Ebner J, *Going Dark: The Secret Social Lives of Extremists* (London: Bloomsbury 2020) 144-145, 260-261.

Eshoo A and Wyden R, ‘Letter to Attorney General Barr’ (US House of Representatives 2019) <https://eshoo.house.gov/media/press-releases/rep-eshoo-sen-wyden-call-attorney-general-stop-requests-weaken-encryption> accessed 3 September 2020.

Farivar C, ‘Apple expands data encryption under iOS 8, making handover to cops moot’ (ArsTechnica 18 September 2014) <https://arstechnica.com/gadgets/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/> accessed 3 September 2020.

Graham L, ‘Hearing on Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy’ (US Committee on the Judiciary 2019) <https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 3 September 2020.

Hall J, ‘Open Letter: Facebook’s End-to-End Encryption Plans’ (Centre for Democracy and Technology 2019) <https://cdt.org/insights/open-letter-facebooks-end-to-end-encryption-plans/> accessed 3 September 2020.

Herpig S and Heumann S, ‘The Encryption Debate in Germany’ (Carnegie Endowment for International Peace 2019) <https://carnegieendowment.org/2019/05/30/encryption-debate-in-germany-pub-79215> accessed 3 September 2020.

Kaye D, ‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression’ A/HRC/29/32 (Office of the United Nations High Commissioner for Human Rights 2015).

Keller M and Dance G, ‘The Internet is Overrun With Images of Child Sexual Abuse. What Went Wrong?’ (New York Times 29 September 2019) <https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html?mtrref=www.google.com&gwh=194FCC964369C8E58858104FA8140A59&gwt=pay&assetType=PAYWALL> accessed 3 September 2020.

Kerr O and Schneier B, ‘Encryption Workarounds’ (2018) 106(4) Georgetown Law Journal 989.

Koomen M, ‘The Encryption Debate in the European Union’ (Carnegie Endowment for International Peace 2019) <https://carnegieendowment.org/2019/05/30/encryption-debate-in-european-union-pub-79220> accessed 3 September 2020.

Kuehn A and McConnell B, *Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions* (EastWest Institute 2018) <https://www.eastwest.ngo/encryption> accessed 3 September 2020.

Landau S, ‘If We Build It (They Will Break In)’ (Lawfare 2020) <https://www.lawfareblog.com/if-we-build-it-they-will-break> accessed 3 September 2020.

Levy I and Robinson C, ‘Principles for a More Informed Exceptional Access Debate’ (Lawfare 2018) <https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate> accessed 3 September 2020.

Liguori C, ‘Exploring Lawful Hacking as a Possible Answer to the “Going Dark” Debate’ (2020) 26 Michigan Technology Law Review 317.

Manpearl E, ‘The International Front of the Going Dark Debate’ (2019) 22(4) Virginia Journal of Law and Technology 158.

McCarthy H, ‘Decoding the encryption debate: why legislating to restrict strong encryption will not resolve the “going dark” problem’ (2016) 20(3) Journal of Internet Law 1.

Mendelsohn T, ‘Secure Boot snafu: Microsoft leaks backdoor key, firmware flung wide open’ (ArsTechnica 11 August 2016) <https://arstechnica.com/information-technology/2016/08/microsoft-secure-boot-firmware-snafu-leaks-golden-key/> accessed 3 September 2020.

Mohanty B, ‘The Encryption Debate in India’ (Carnegie Endowment for International Peace 2019) <https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213> accessed 3 September 2020.

Neuenschwander E, ‘Testimony for Hearing on Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy’ (US Committee on the Judiciary 2019) <https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 3 September 2020.

Nicas J and Benner K, ‘F.B.I. Asks Apple to Help Unlock Two iPhones’ (New York Times 7 January 2020) <https://www.nytimes.com/2020/01/07/technology/apple-fbi-iphone-encryption.html> accessed 3 September 2020.

Patel P, ‘Facebook’s encryption could stop our police doing their job properly - and I won’t allow that to happen’ (The Telegraph 30 July 2019) <https://www.telegraph.co.uk/politics/2019/07/30/facebooks-encryption-could-stop-police-job-properly-wont-allow/> accessed 3 September 2020.

Patel P, Barr W, McAleenan K and Dutton P, ‘Open Letter: Facebook’s “Privacy First” Proposals’ (UK Government 2019) <https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg> accessed 3 September 2020 (Open Letter to Facebook).

Patel P, Barr W and Dutton P, ‘Remarks for Lawful Access Summit’ (United States Department of Justice 2019) at 3:55:00 <https://www.justice.gov/opa/video/lawful-access-summit> accessed 3 September 2020.

Perlroth N and Shane S, ‘In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc’ (New York Times 25 May 2019) <https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html> accessed 3 September 2020.

Pfefferkorn R, ‘Banning Strong Encryption Does Not Mean Catching Criminals. It Only Makes You Less Safe From Them’ (Stanford Centre for Internet and Society 2019) <http://cyberlaw.stanford.edu/blog/2019/11/banning-strong-encryption-does-not-mean-catching-criminals-it-only-makes-you-less-safe> accessed 3 September 2020.

Pfefferkorn R, ‘The EARN IT Act: How to Ban End-to-End Encryption Without Actually Banning It’ (Stanford Centre for Internet and Society 2020) <http://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it> accessed 3 September 2020.

Pfefferkorn R, ‘The EARN IT Act Threatens Our Online Freedoms. New Amendments Don’t Fix It’ (Stanford Centre for Internet and Society 2020) <http://cyberlaw.stanford.edu/blog/2020/07/earn-it-act-threatens-our-online-freedoms-new-amendments-don%E2%80%99t-fix-it> accessed 3 September 2020.

Rozenshtein A, ‘Surveillance Intermediaries’ (2018) 70 Stanford Law Review 99.

Rozenshtein A, ‘Wicked Crypto’ (2019) 9 UC Irvine Law Review 1181.

Rozenshtein A, ‘Congress, Not the Attorney General, Should Decide the Future of Encryption’ (Lawfare 2020) <https://www.lawfareblog.com/congress-not-attorney-general-should-decide-future-encryption> accessed 3 September 2020.

Savage C, ‘F.B.I. Admits Overstating Locked Phone Problem, and Critics Pounce’ (New York Times 23 May 2018) <https://www.nytimes.com/2018/05/23/us/politics/fbi-going-dark-cellphones-total-overstated.html> accessed 3 September 2020.

Schneier B, ‘Evaluating the GCHQ Exceptional Access Proposal’ (Lawfare 2019) <https://www.lawfareblog.com/evaluating-gchq-exceptional-access-proposal> accessed 3 September 2020.

Schneier B, ‘Attorney General William Barr on Encryption Policy’ (Lawfare 2019) <https://www.lawfareblog.com/attorney-general-william-barr-encryption-policy> accessed 3 September 2020.

Squires C, ‘Written Testimony for Judiciary Committee United States Senate hearing: Encryption and Lawful Access’ (UK Government 2019) <https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg/written-testimony-of-chloe-squires-director-national-security-home-office> accessed 3 September 2019.

Stilgherrian, ‘The Encryption Debate in Australia’ (Carnegie Endowment for International Peace 2019) <https://carnegieendowment.org/2019/05/30/encryption-debate-in-australia-pub-79217> accessed 3 September 2020.

Sullivan J, ‘Testimony for Hearing on Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy’ (US Committee on the Judiciary 2019) <https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 3 September 2020.

Sullivan J, ‘Preventing Unwanted Contacts and Scams in Messenger’ (Facebook 2020) <https://messengernews.fb.com/2020/05/21/preventing-unwanted-contacts-and-scams-in-messenger/> accessed 3 September 2020.

Tait M, ‘Testimony for Hearing on Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy’ (US Committee on the Judiciary 2019) <https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 3 September 2020.

Timm T, ‘The “Athens Affair” shows why we need encryption without backdoors’ (The Guardian 30 September 2015) <https://www.theguardian.com/commentisfree/2015/sep/30/athens-affair-encryption-backdoors> accessed 3 September 2020.

Vance C, ‘Testimony for Hearing on Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy’ (US Committee on the Judiciary 2019) <https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 3 September 2020.

Vance C, ‘Response to Questions for Hearing on Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy’ (US Committee on the Judiciary 2019) <https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 3 September 2020.

Watt N, Mason R and Traynor I, ‘David Cameron pledges anti-terror law for internet after Paris attacks’ (The Guardian 12 January 2015) <https://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg> accessed 3 September 2020.

Wray C, ‘Remarks for Lawful Access Summit’ (United States Department of Justice 2019) <https://www.justice.gov/opa/video/lawful-access-summit> accessed 3 September 2020.

Yadron D, ‘San Bernardino iPhone: US ends Apple case after accessing data without assistance’ (The Guardian 29 March 2016) <https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone> accessed 3 September 2020.

Zittrain J, Olsen M, O’Brien D and Schneier B, ‘Don’t Panic: Making Progress on the “Going Dark” Debate’ (Berkman Centre Research Publication 2016) <https://dash.harvard.edu/handle/1/28552576> accessed 3 September 2020.

Zuckerberg M, ‘A Privacy-Focused Vision for Social Networking’ (Facebook 2019) <https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/> accessed 3 September 2020.

1. Carlos Liguori, ‘Exploring Lawful Hacking as a Possible Answer to the “Going Dark” Debate’ (2020) 26 Michigan Technology Law Review 317, 324. [↑](#footnote-ref-1)
2. See for example Ian Levy and Crispin Robinson, ‘Principles for a More Informed Exceptional Access Debate’ (Lawfare 2018) <https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate> accessed 3 September 2020 (Ghost Proposal); Christopher Wray, ‘Remarks for Lawful Access Summit’ (United States Department of Justice 2019) <https://www.justice.gov/opa/video/lawful-access-summit> accessed 3 September 2020; Cyrus Vance, ‘Testimony for Hearing on Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy’ (US Committee on the Judiciary 2019) <https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 3 September 2020. [↑](#footnote-ref-2)
3. Will Cathcart and Stan Chudnovsky, ‘Facebook’s Public Response to Open Letter on Private Messaging’ (Facebook 2019) <https://about.fb.com/news/2019/12/facebooks-response-to-open-letter-on-private-messaging/> accessed 3 September 2020 (Facebook’s Open Letter); Joseph Lorenzo Hall, ‘Open Letter: Facebook’s End-to-End Encryption Plans’ (Centre for Democracy and Technology 2019) <https://cdt.org/insights/open-letter-facebooks-end-to-end-encryption-plans/> accessed 3 September 2020. [↑](#footnote-ref-3)
4. Jonathan Zittrain, Matthew Olsen, David O’Brien and Bruce Schneier, ‘Don’t Panic: Making Progress on the “Going Dark” Debate’ (Berkman Centre Research Publication 2016) <https://dash.harvard.edu/handle/1/28552576> accessed 3 September 2020; Alan Rozenshtein, ‘Wicked Crypto’ (2019) 9 UC Irvine Law Review 1181. [↑](#footnote-ref-4)
5. David Kaye, ‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression’ A/HRC/29/32 (Office of the United Nations High Commissioner for Human Rights 2015). [↑](#footnote-ref-5)
6. Jim Baker, ‘Rethinking Encryption’ (Lawfare 2019) <https://www.lawfareblog.com/rethinking-encryption> accessed 3 September 2020. [↑](#footnote-ref-6)
7. Ghost Proposal (n 2). For criticism see Bruce Schneier, ‘Evaluating the GCHQ Exceptional Access Proposal’ (Lawfare 2019) <https://www.lawfareblog.com/evaluating-gchq-exceptional-access-proposal> accessed 3 September 2020; Sharon Bradford Franklin and Andi Wilson Thompson, ‘Open Letter to GCHQ on the Threats Posed by the Ghost Proposal’ (Lawfare 2019) <https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal> accessed 3 September 2020. [↑](#footnote-ref-7)
8. Andreas Kuehn and Bruce McConnell, *Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions* (EastWest Institute 2018) <https://www.eastwest.ngo/encryption> accessed 3 September 2020 (EastWest Institute); Liguori (n 1). [↑](#footnote-ref-8)
9. Princeton University Centre For Information Technology Policy and Carnegie Endowment for International Peace, ‘Implications of Quantum Computing for Encryption Policy’ (Carnegie Endowment 2019) <https://carnegieendowment.org/2019/04/25/implications-of-quantum-computing-for-encryption-policy-pub-78985> accessed 3 September 2020. [↑](#footnote-ref-9)
10. Privacy International, ‘Five Eyes’ (Privacy International) <https://privacyinternational.org/learn/five-eyes> accessed 3 September 2020. [↑](#footnote-ref-10)
11. Hugh McCarthy, ‘Decoding the encryption debate: why legislating to restrict strong encryption will not resolve the “going dark” problem’ (2016) 20(3) Journal of Internet Law 1, 19-20. [↑](#footnote-ref-11)
12. Ibid 20-21. [↑](#footnote-ref-12)
13. Regulation of Investigatory Powers Act 2000 pt III (RIPA). [↑](#footnote-ref-13)
14. Privacy International (n 10). [↑](#footnote-ref-14)
15. The Guardian, *‘The NSA Files’* (The Guardian) <https://www.theguardian.com/us-news/the-nsa-files> accessed 3 September 2020; Mark Zuckerberg, ‘A Privacy-Focused Vision for Social Networking’ (Facebook 2019) <https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/> accessed 3 September 2020. [↑](#footnote-ref-15)
16. Orin Kerr and Bruce Schneier, ‘Encryption Workarounds’ (2018) 106(4) Georgetown Law Journal 989, 993-995. [↑](#footnote-ref-16)
17. Cyrus Farivar, ‘Apple expands data encryption under iOS 8, making handover to cops moot’ (ArsTechnica 18 September 2014) <https://arstechnica.com/gadgets/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/> accessed 3 September 2020. [↑](#footnote-ref-17)
18. Tim Cook, ‘A Message to Our Customers’ (Apple 2016) <https://www.apple.com/customer-letter/> accessed 3 September 2020; Jack Nicas and Katie Benner, ‘F.B.I. Asks Apple to Help Unlock Two iPhones’ (New York Times 7 January 2020) <https://www.nytimes.com/2020/01/07/technology/apple-fbi-iphone-encryption.html> accessed 3 September 2020. [↑](#footnote-ref-18)
19. Eric Manpearl, ‘The International Front of the Going Dark Debate’ (2019) 22(4) Virginia Journal of Law and Technology 158, 208, 216. [↑](#footnote-ref-19)
20. Sven Herpig and Stefan Heumann, ‘The Encryption Debate in Germany’ (Carnegie Endowment for International Peace 2019) <https://carnegieendowment.org/2019/05/30/encryption-debate-in-germany-pub-79215> accessed 3 September 2020; Liguori (n 1) 336-338. [↑](#footnote-ref-20)
21. Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018. [↑](#footnote-ref-21)
22. Stilgherrian, ‘The Encryption Debate in Australia’ (Carnegie Endowment for International Peace 2019) <https://carnegieendowment.org/2019/05/30/encryption-debate-in-australia-pub-79217> accessed 3 September 2020; Liguori (n 1) 340-342. [↑](#footnote-ref-22)
23. Gabriel Aleixo, Andrea Guimaraes Gobbato, Isabela Garcia De Souza, Natalia Langenegger, Ronaldo Lemos and Fabro Steibel, ‘The Encryption Debate in Brazil’ (Carnegie Endowment for International Peace 2019) <https://carnegieendowment.org/2019/05/30/encryption-debate-in-brazil-pub-79219> accessed 3 September 2020; Maria Koomen, ‘The Encryption Debate in the European Union’ (Carnegie Endowment for International Peace 2019) <https://carnegieendowment.org/2019/05/30/encryption-debate-in-european-union-pub-79220> accessed 3 September 2020; Bedavyasa Mohanty, ‘The Encryption Debate in India’ (Carnegie Endowment for International Peace 2019) <https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213> accessed 3 September 2020. [↑](#footnote-ref-23)
24. Investigatory Powers Act 2016 s 253. [↑](#footnote-ref-24)
25. Investigatory Powers (Technical Capability) Regulations 2018. [↑](#footnote-ref-25)
26. Baker (n 6). [↑](#footnote-ref-26)
27. Zuckerberg (n 15). [↑](#footnote-ref-27)
28. Jay Sullivan, ‘Testimony for Hearing on Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy’ (US Committee on the Judiciary 2019) 5 <https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 3 September 2020. [↑](#footnote-ref-28)
29. William Barr, ‘Keynote Address’ (International Conference on Cyber Security at Fordham University 2019) <https://www.lawfareblog.com/attorney-general-delivers-address-encryption-cybersecurity-conference> accessed 3 September 2020. [↑](#footnote-ref-29)
30. Priti Patel, William Barr, Kevin McAleenan and Peter Dutton, ‘Open Letter: Facebook’s “Privacy First” Proposals’ (UK Government 2019) <https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg> accessed 3 September 2020 (Open Letter to Facebook); Priti Patel, William Barr and Peter Dutton, ‘Remarks for Lawful Access Summit’ (United States Department of Justice 2019) at 3:55:00 <https://www.justice.gov/opa/video/lawful-access-summit> accessed 3 September 2020. [↑](#footnote-ref-30)
31. US Senate 116th Congress *S 3398 Eliminating Abusive and Rampant Neglect of Interactive Technologies Act* (Washington: Government Printing Office 2020). [↑](#footnote-ref-31)
32. Alan Rozenshtein, ‘Congress, Not the Attorney General, Should Decide the Future of Encryption’ (Lawfare 2020) <https://www.lawfareblog.com/congress-not-attorney-general-should-decide-future-encryption> accessed 3 September 2020. [↑](#footnote-ref-32)
33. Riana Pfefferkorn, ‘The EARN IT Act Threatens Our Online Freedoms. New Amendments Don’t Fix It’ (Stanford Centre for Internet and Society 2020) <http://cyberlaw.stanford.edu/blog/2020/07/earn-it-act-threatens-our-online-freedoms-new-amendments-don%E2%80%99t-fix-it> accessed 3 September 2020. [↑](#footnote-ref-33)
34. US Senate 116th Congress *S 4051 Lawful Access to Encrypted Data Act* (Washington: Government Printing Office 2020); Andrew Crocker, ‘The Senate’s New Anti-Encryption Bill Is Even Worse Than EARN IT, and That’s Saying Something’ (Electronic Frontier Foundation 2020) <https://www.eff.org/deeplinks/2020/06/senates-new-anti-encryption-bill-even-worse-earn-it-and-thats-saying-something> accessed 3 September 2020. [↑](#footnote-ref-34)
35. Open Letter to Facebook (n 30). [↑](#footnote-ref-35)
36. Ibid. [↑](#footnote-ref-36)
37. National Society for the Prevention of Cruelty to Children, ‘Our letter to Facebook’ (National Society for the Prevention of Cruelty to Children 2019) <https://www.nspcc.org.uk/about-us/news-opinion/2019/facebook-encryption-sexual-abuse/> accessed 3 September 2020. [↑](#footnote-ref-37)
38. Sullivan (n 28) 4. [↑](#footnote-ref-38)
39. Kerr and Schnier (n 16) 1013. [↑](#footnote-ref-39)
40. Anna Eshoo and Ron Wyden, ‘Letter to Attorney General Barr’ (US House of Representatives 2019) <https://eshoo.house.gov/media/press-releases/rep-eshoo-sen-wyden-call-attorney-general-stop-requests-weaken-encryption> accessed 3 September 2020. [↑](#footnote-ref-40)
41. Sullivan (n 28) 5. [↑](#footnote-ref-41)
42. McCarthy (n 11) 23; Riana Pfefferkorn, ‘Banning Strong Encryption Does Not Mean Catching Criminals. It Only Makes You Less Safe From Them’ (Stanford Centre for Internet and Society 2019) <http://cyberlaw.stanford.edu/blog/2019/11/banning-strong-encryption-does-not-mean-catching-criminals-it-only-makes-you-less-safe> accessed 3 September 2020. [↑](#footnote-ref-42)
43. Julia Ebner, *Going Dark: The Secret Social Lives of Extremists* (London: Bloomsbury 2020) 144-145, 260-261. [↑](#footnote-ref-43)
44. Kaye (n 5) 12-15. [↑](#footnote-ref-44)
45. Charlie Savage, ‘F.B.I. Admits Overstating Locked Phone Problem, and Critics Pounce’ (New York Times 23 May 2018) <https://www.nytimes.com/2018/05/23/us/politics/fbi-going-dark-cellphones-total-overstated.html> accessed 3 September 2020. [↑](#footnote-ref-45)
46. Cyrus Vance, ‘Response to Questions for Hearing on Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy’ (US Committee on the Judiciary 2019) <https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 3 September 2020. [↑](#footnote-ref-46)
47. Charles Duan, Arthur Rizer, Zach Graves and Mike Godwin, ‘Policy Approaches to the Encryption Debate’ (R Street Institute 2018) 5 <https://www.rstreet.org/2018/03/05/policy-approaches-to-the-encryption-debate/> accessed 3 September 2020. [↑](#footnote-ref-47)
48. Zitrain, Olsen, O’Brien and Schnier (n 4). [↑](#footnote-ref-48)
49. Kaye (n 5) 4. [↑](#footnote-ref-49)
50. Facebook’s Open Letter (n 3); Sullivan (n 28) 5. [↑](#footnote-ref-50)
51. Hall (n 3). [↑](#footnote-ref-51)
52. Sullivan (n 28) 5. [↑](#footnote-ref-52)
53. William Barr, ‘Panel at Lawful Access Summit’ (United States Department of Justice 2019) at [04:18:10] <https://www.justice.gov/opa/video/lawful-access-summit> accessed 3 September 2020. [↑](#footnote-ref-53)
54. McCarthy (n 11) 24; Manpearl (n 19) 223-227; Alan Rozenshtein, ‘Surveillance Intermediaries’ (2018) 70 Stanford Law Review 99, 117. [↑](#footnote-ref-54)
55. McCarthy (n 11) 33-34. [↑](#footnote-ref-55)
56. Joint Committee on the Draft Investigatory Powers Bill, ‘Volume of Written Evidence’ (UK Parliament 2016) 387-388 <https://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-investigatory-powers-bill/publications/> accessed 3 September 2020. [↑](#footnote-ref-56)
57. Barr (n 29); William Barr, ‘Remarks as Prepared for Delivery at Lawful Access Summit’ (US Department of Justice 2019) <https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-lawful-access-summit> accessed 3 September 2020. [↑](#footnote-ref-57)
58. Baker (n 6). [↑](#footnote-ref-58)
59. Eric Neuenschwander, ‘Testimony for Hearing on Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy’ (US Committee on the Judiciary 2019) <https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 3 September 2020. [↑](#footnote-ref-59)
60. Baker (n 6); Neuenschwander (n 59), Sullivan (n 28) 1. [↑](#footnote-ref-60)
61. Carnegie Encryption Working Group, ‘Moving the Encryption Policy Conversation Forward’ (Carnegie Endowment for International Peace 2019) <https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573> accessed 3 September 2020. [↑](#footnote-ref-61)
62. Kaye (n 5) 5-6. [↑](#footnote-ref-62)
63. Zuckerberg (n 15). [↑](#footnote-ref-63)
64. Barr (n 29); Barr, Remarks for Lawful Access Summit (n 57). [↑](#footnote-ref-64)
65. Bruce Schneier, ‘Attorney General William Barr on Encryption Policy’ (Lawfare 2019) <https://www.lawfareblog.com/attorney-general-william-barr-encryption-policy> accessed 3 September 2020. [↑](#footnote-ref-65)
66. Eshoo and Wyden (n 40). [↑](#footnote-ref-66)
67. Sullivan (n 28) 2. [↑](#footnote-ref-67)
68. Communications Assistance for Law Enforcement Act 1994. [↑](#footnote-ref-68)
69. Susan Landau, ‘If We Build It (They Will Break In)’ (Lawfare 2020) <https://www.lawfareblog.com/if-we-build-it-they-will-break> accessed 3 September 2020. [↑](#footnote-ref-69)
70. Ibid. [↑](#footnote-ref-70)
71. Trevor Timm, ‘The “Athens Affair” shows why we need encryption without backdoors’ (The Guardian 30 September 2015) <https://www.theguardian.com/commentisfree/2015/sep/30/athens-affair-encryption-backdoors> accessed 3 September 2020. [↑](#footnote-ref-71)
72. Tom Mendelsohn, ‘Secure Boot snafu: Microsoft leaks backdoor key, firmware flung wide open’ (ArsTechnica 11 August 2016) <https://arstechnica.com/information-technology/2016/08/microsoft-secure-boot-firmware-snafu-leaks-golden-key/> accessed 3 September 2020. [↑](#footnote-ref-72)
73. Nicole Perlroth and Scott Shane, ‘In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc’ (New York Times 25 May 2019) <https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html> accessed 3 September 2020. [↑](#footnote-ref-73)
74. Landau (n 69). For further examples see Duan, Rizen, Graves and Godwin (n 47) 9-11. [↑](#footnote-ref-74)
75. Chloe Squires, ‘Written Testimony for Judiciary Committee United States Senate hearing: Encryption and Lawful Access’ (UK Government 2019) 13 <https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg/written-testimony-of-chloe-squires-director-national-security-home-office> accessed 3 September 2019. [↑](#footnote-ref-75)
76. Ghost Proposal (n 2); Schneier (n 7); Bradford Franklin and Wilson Thompson (n 7). [↑](#footnote-ref-76)
77. Duan, Rizer, Graves and Godwin (n 47) 10. [↑](#footnote-ref-77)
78. Ghost Proposal (n 2). [↑](#footnote-ref-78)
79. Five Eyes Country Ministerial communiques, ‘Joint meeting of Five Country Ministerial and quintet of Attorneys-General: communique, London 2019’ (UK Government 2019) <https://www.gov.uk/government/publications/five-country-ministerial-communique> accessed 3 September 2020. [↑](#footnote-ref-79)
80. Squires (n 75) 1. [↑](#footnote-ref-80)
81. Barr (n 29). [↑](#footnote-ref-81)
82. Wray (n 2) at [00:13:45]. [↑](#footnote-ref-82)
83. Duan, Rizer, Graves and Godwin (n 47) 6-7. [↑](#footnote-ref-83)
84. Wray (n 2) at [00:07:40]. [↑](#footnote-ref-84)
85. Squires (n 75) 3; Vance (n 2) 1. [↑](#footnote-ref-85)
86. Priti Patel, ‘Panel at Lawful Access Summit’ (United States Department of Justice 2019) at [4:09:00] <https://www.justice.gov/opa/video/lawful-access-summit> accessed 3 September 2020. [↑](#footnote-ref-86)
87. Baker (n 6). [↑](#footnote-ref-87)
88. Zuckerberg (n 15). [↑](#footnote-ref-88)
89. Baker (n 6). [↑](#footnote-ref-89)
90. Kerr and Schnier (n 16) 1010-1011. [↑](#footnote-ref-90)
91. Princeton University Centre For Information Technology Policy and Carnegie Endowment for International Peace, ‘Likely Future Adoption of User-Controlled Encryption’ (Carnegie Endowment 2019) <https://carnegieendowment.org/2019/04/25/likely-future-adoption-of-user-controlled-encryption-pub-78986> accessed 3 September 2020. [↑](#footnote-ref-91)
92. Vance (n 2) 6-7. [↑](#footnote-ref-92)
93. Zittrain, Olsen, O’Brien and Schneier (n 4) 9-13; Princeton University and Carnegie Group (n 91). [↑](#footnote-ref-93)
94. For examples of lawful hacking being proposed as a complete solution see Liguori (n 1) and EastWest Institute (n 8). [↑](#footnote-ref-94)
95. Kerr and Schnier (n 16). [↑](#footnote-ref-95)
96. Matt Tait, ‘Testimony for Hearing on Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy’ (US Committee on the Judiciary 2019) <https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 3 September 2020. [↑](#footnote-ref-96)
97. Danny Yadron, ‘San Bernardino iPhone: US ends Apple case after accessing data without assistance’ (The Guardian 29 March 2016) <https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone> accessed 3 September 2020; Thomas Brewster, ‘FBI Hacks iPhones In Pensacola Terrorist Shooting Case, But the War With Apple Goes On’ (Forbes 18 May 2020) <https://www.forbes.com/sites/thomasbrewster/2020/05/18/feds-hack-iphones-in-pensacola-case-apple-not-needed-after-all/#9491dcb75e99> accessed 3 September 2020. [↑](#footnote-ref-97)
98. Herpig and Heumann (n 20). [↑](#footnote-ref-98)
99. Vance (n 2) 4-5. [↑](#footnote-ref-99)
100. Baker (n 6); Ghost Proposal (n 2); Rozenshtein (n 54) 170. [↑](#footnote-ref-100)
101. Liguori (n 1) 334-336. [↑](#footnote-ref-101)
102. Kerr and Schnier (n 16) 1018. [↑](#footnote-ref-102)
103. Suan, Rizer, Graves, and Godwin (n 47) 9-10; Carnegie Encryption Working Group (n 61). [↑](#footnote-ref-103)
104. Vance (n 2) 4. [↑](#footnote-ref-104)
105. Carnegie Encryption Working Group (n 61); Baker (n 6). [↑](#footnote-ref-105)
106. Facebook’s Open Letter (n 3); Sullivan (n 28) 3-6; Jay Sullivan, ‘Preventing Unwanted Contacts and Scams in Messenger’ (Facebook 2020) <https://messengernews.fb.com/2020/05/21/preventing-unwanted-contacts-and-scams-in-messenger/> accessed 3 September 2020. [↑](#footnote-ref-106)
107. Duan, Rizer, Graves and Godwin (n 47) 12; Baker (n 6). [↑](#footnote-ref-107)
108. Ghost Proposal (n 2) principle two. [↑](#footnote-ref-108)
109. Princeton University and Carnegie Endowment (n 9). [↑](#footnote-ref-109)
110. Rozenshtein (n 4) 1196-1197, 1211-1212. [↑](#footnote-ref-110)
111. The Home Office and Priti Patel, ‘Home Secretary chairs virtual ‘Five Eyes’ security summit’ (UK Government 2020) <https://www.gov.uk/government/news/home-secretary-chairs-virtual-five-eyes-security-summit> accessed 3 September 2020. [↑](#footnote-ref-111)
112. Priti Patel, ‘Facebook’s encryption could stop our police doing their job properly - and I won’t allow that to happen’ (The Telegraph 30 July 2019) <https://www.telegraph.co.uk/politics/2019/07/30/facebooks-encryption-could-stop-police-job-properly-wont-allow/> accessed 3 September 2020. [↑](#footnote-ref-112)
113. Investigatory Powers Act 2016 s 255(8). [↑](#footnote-ref-113)
114. Barr (n 29). See also Barr (n 57). [↑](#footnote-ref-114)
115. Lindsey Graham, ‘Hearing on Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy’ (US Committee on the Judiciary 2019) at [00:21:50] <https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 3 September 2020. [↑](#footnote-ref-115)
116. EARN IT Act (n 31); Rozenshtein (n 32). [↑](#footnote-ref-116)
117. Pfefferkorn (n 33). [↑](#footnote-ref-117)
118. LAED Act (n 34); Crocker (n 34). [↑](#footnote-ref-118)
119. EastWest Institute (n 8) 4. [↑](#footnote-ref-119)
120. Carnegie Encryption Working Group (n 61). [↑](#footnote-ref-120)
121. Barr (n 29). [↑](#footnote-ref-121)
122. Patel (n 86) at [4:29:00]. [↑](#footnote-ref-122)
123. Investigatory Powers Act 2016. [↑](#footnote-ref-123)
124. EARN IT Act (n 31). [↑](#footnote-ref-124)
125. Communications Decency Act 1996 s 230. [↑](#footnote-ref-125)
126. Squires (n 75) 6-7. [↑](#footnote-ref-126)
127. Squires (n 75) 7. [↑](#footnote-ref-127)
128. Investigatory Powers Act s 255. [↑](#footnote-ref-128)
129. Squires (n 75) 9-10. [↑](#footnote-ref-129)
130. HL Deb 13 July 2016, vol 774 at <https://bit.ly/2Dr8ldQ>; <https://bit.ly/351KPiS>; <https://bit.ly/2QYG9C5>. [↑](#footnote-ref-130)
131. HL Deb 19 October 2016, vol 774 at <https://bit.ly/2ZPxAME>. [↑](#footnote-ref-131)
132. Ibid at <https://bit.ly/2Z5FIdU>. [↑](#footnote-ref-132)
133. Joint Committee on the Draft Investigatory Powers Bill (n 56) 398-390. [↑](#footnote-ref-133)
134. HC Deb 3 May 2016, vol 609, col 645 at <https://bit.ly/3i1RjC8>. [↑](#footnote-ref-134)
135. Investigatory Powers (Technical Capability) Regulations 2018 sch 1 s 8 and sch 2 s 9. [↑](#footnote-ref-135)
136. Squires (n 75) 9. [↑](#footnote-ref-136)
137. EARN IT Act (n 31). [↑](#footnote-ref-137)
138. Communications Decency Act 1996 s230. [↑](#footnote-ref-138)
139. Zoe Bedell and John Major, ‘What’s Next for Section 230? A Roundup of Proposals’ (Lawfare 2020) <https://www.lawfareblog.com/whats-next-section-230-roundup-proposals> accessed 3 September 2020. [↑](#footnote-ref-139)
140. EARN IT Act (n 31). [↑](#footnote-ref-140)
141. Riana Pfefferkorn, ‘The EARN IT Act: How to Ban End-to-End Encryption Without Actually Banning It’ (Stanford Centre for Internet and Society 2020) <http://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it> accessed 3 September 2020. [↑](#footnote-ref-141)
142. Communications Assistance for Law Enforcement Act 1994. [↑](#footnote-ref-142)
143. 47 USC § 1002(b)(3). [↑](#footnote-ref-143)
144. Pfefferkorn (n 141). [↑](#footnote-ref-144)
145. Pfefferkorn (n 42). [↑](#footnote-ref-145)
146. See for example Squires (n 75) 4-5. [↑](#footnote-ref-146)
147. Vance (n 2). [↑](#footnote-ref-147)
148. Barr (n 29). [↑](#footnote-ref-148)
149. Home Office and Patel (n 111); Barr (n 29); Patel July 2019 (n 112). [↑](#footnote-ref-149)
150. Eshoo and Wyden (n 40); Pfefferkorn (n 42); Baker (n 6). [↑](#footnote-ref-150)
151. Eshoo and Wyden (n 40). [↑](#footnote-ref-151)
152. Michael Keller and Gabriel Dance, ‘The Internet is Overrun With Images of Child Sexual Abuse. What Went Wrong?’ (New York Times 29 September 2019) <https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html?mtrref=www.google.com&gwh=194FCC964369C8E58858104FA8140A59&gwt=pay&assetType=PAYWALL> accessed 3 September 2020. [↑](#footnote-ref-152)
153. Baker (n 6). [↑](#footnote-ref-153)
154. Pfefferkorn (n 141). [↑](#footnote-ref-154)
155. Barr (n 29). [↑](#footnote-ref-155)
156. Patel (n 112). [↑](#footnote-ref-156)
157. Five Eyes (n 79). [↑](#footnote-ref-157)
158. Squires (n 75) 4-5; Open Letter to Facebook (n 30). [↑](#footnote-ref-158)
159. Open letter to Facebook (n 30); National Society for the Prevention of Cruelty to Children (n 37). [↑](#footnote-ref-159)
160. Wray (n 2) at [00:14:40]. [↑](#footnote-ref-160)
161. Nicholas Watt, Rowena Mason and Ian Traynor, ‘David Cameron pledges anti-terror law for internet after Paris attacks’ (The Guardian 12 January 2015) <https://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg> accessed 3 September 2020. [↑](#footnote-ref-161)
162. Barr (n 29). [↑](#footnote-ref-162)
163. Wray (n 2) at [00:10:00]. [↑](#footnote-ref-163)
164. Patel (n 86) at [3:59:00]. [↑](#footnote-ref-164)
165. Graham (n 115) at [00:21:30]. [↑](#footnote-ref-165)
166. Keller and Dance (n 152). [↑](#footnote-ref-166)
167. National Society for the Prevention of Cruelty to Children (n 37). [↑](#footnote-ref-167)
168. HC Deb 3 May 2016, vol 609, col 646. [↑](#footnote-ref-168)
169. Lawful Access to Encrypted Data Act (n 34) s 601. [↑](#footnote-ref-169)
170. Ibid. [↑](#footnote-ref-170)
171. Investigatory Powers Act 2016 s 253(3). [↑](#footnote-ref-171)
172. Hence the purpose of Investigatory Powers Act 2016 s 253(1). [↑](#footnote-ref-172)
173. Investigatory Powers Act 2016. [↑](#footnote-ref-173)
174. HC Deb 3 May 2016, vol 609, col 645 at <https://bit.ly/3i1RjC8>. [↑](#footnote-ref-174)
175. UK Parliament, ‘Investigatory Powers Bill: Written Evidence submitted by Apple Inc, Facebook Inc, Google Inc, Microsoft Corp, Twitter Inc and Yahoo Inc’ (UK Parliament 2016) <https://publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB21.htm> accessed 3 September 2020. [↑](#footnote-ref-175)
176. Squires (n 75) 2-3. [↑](#footnote-ref-176)
177. Barr (n 29). Barr (n 57). [↑](#footnote-ref-177)
178. Vance (n 2). [↑](#footnote-ref-178)
179. Wray (n 2) at [00:11.40]. See also Patel at [3:59:00]. [↑](#footnote-ref-179)