Written Testimony of

Chloe Squires
Director National Security
United Kingdom Home Office

Judiciary Committee United States Senate hearing:
Encryption and Lawful Access:
Evaluating Benefits and Risks to Public Safety and Privacy
December 10, 2019

1. I welcome the opportunity to provide a written testimony on behalf of the United Kingdom Government in support of the Committee's hearing: "Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy".

2. In this statement I set out the UK Government's policy position in relation to targeted law enforcement and intelligence agency access to encrypted communications. In doing so, I hope to achieve three things. First, to make clear why this is such an important issue for the UK Government, highlighting the very significant impact on our law enforcement and intelligence agencies where companies design their services in such a way that they cannot access the content of communications, even in relation to the most serious crimes. Second, to demonstrate that our position on this issue is balanced and underpinned by strong legislation and reasonable policies. Third, to address a number of misconceptions about how our approach relates to cyber security and privacy.

3. The UK Government supports strong encryption and understands its importance for a free, open and secure internet and as part of creating a strong digital economy. We believe encryption is a necessary part of protecting our citizens' data online and billions of people use it every day for a range of services including banking, commerce and communications. We do not want to compromise the wider safety or security of digital products and services for law abiding users or impose solutions on technology companies that may not work within their complex systems.

4. However, as more and more of our lives move online, we need to try and ensure our law enforcement and intelligence agencies retain the ability to gain lawful access to the communications of criminals and other individuals who threaten public safety where that is necessary to progress their investigations. There is a particular challenge where companies design their services in such a way that even they cannot see the content of their users' communications. Increasingly, this is a challenge shared between governments who have a responsibility to protect their citizens and the tech companies that facilitate those citizens' lives online. We believe that the only way to make progress on this shared challenge is to engender an ongoing, open and transparent dialogue between these groups and other interested parties, focusing on reasonable proposals and respecting everyone's core values.

5. This statement builds on an article published in November 2018 on the national security blog, Lawfare. That article: "Principles for a More Informed Exceptional Access Debate" was written by the Technical Director of the National Cyber Security Centre in the UK, Ian Levy, and the then Technical Director of Cryptanalysis at the Government Communications Headquarters (GCHQ), Crispin Robinson[1]. In it they set out six core principles that the UK Government is using to frame our engagement with industry in relation to lawful access. Everything that I say in this statement should be read in the context of, and in conjunction with, their article. As set out in that article, the principles do not cover how the Government may access data in every case, nor do they address the "discovery" problem about how governments establish what services and identities are being used by criminals and other valid targets. The principles are specifically for mass scale, commodity, end-to-end encrypted services. In this context, we refer to "lawful access" as meaning a targeted Government authorisation to access the data of an individual with the assistance of the service provider in the exceptionally limited circumstances where it is necessary and proportionate to prevent or detect serious crime or protect national security.

6. My intention is to reinforce the points made in the Lawfare article, not to repeat them, and to continue the conversation that article started. I will do that by setting out further context about how the principles fit with the UK's wider policy position and legal framework on lawful access. That position is not about any one company. However, this testimony should also be read in the context of the open letter to Mark Zuckerberg of 4 October 2019, signed by the Home Secretary, alongside the United States Attorney General William Barr, then Acting Secretary of Homeland Security Kevin McAleenan, and the Australian Minister for Home Affairs Peter Dutton. That letter makes very clear the severe potential impact on public safety of Facebook's current proposals to move their three core messaging services to end-to-end encryption.

7. The risks to public safety where encryption precludes the needs of law enforcement, including targeted access to content, are grave. That impact is felt in two distinct areas. Firstly, by inhibiting the ability of law enforcement agencies to access content in exceptional circumstances where that is necessary and proportionate to investigate serious crime and protect national security, and where an interception warrant for that purpose has been lawfully issued. Secondly, by diminishing a company's own ability to identify and tackle the most serious illegal content and activity running over its platform, including grooming, indecent imagery of children, terrorist propaganda and attack planning.

Lawful access:

8. In relation to lawful access, the interception of communications is a critical power available to a very limited number of operational agencies in the UK, in order to prevent and detect serious crime and defend national security, including protecting our citizens from terrorism. The large majority of interception warrants issued in the interests of serious crime relate to the unlawful supply of controlled drugs, firearms offences, financial crime such as money laundering, armed robbery and

[1] https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate

human trafficking. The ability of our law enforcement agencies to prevent, detect and investigate such harmful crimes effectively through their use of interception is vital to ensuring public safety and regularly saves lives.

9. In these cases, the use of interception powers specifically to gain access to the content of communications – as opposed to being able only to access others forms of information such as metadata – is critical to securing effective investigative outcomes. The content of messages reveals operational details of the activities subjects of interest carry out in order to facilitate terrorism or other serious crimes, such as meeting with conspirators or procuring materials or weapons needed for the crime or attack. Without this context, investigators will be unable to determine whether to take further action given that the fact of contact between a potential subject of interest and another individual cannot, in itself, indicate involvement in criminality, conspiracy or even sympathy with the subject of interest's terrorist or other criminal activity. Access to content can also provide unique insight into the intention and mind-set of what a subject of interest is planning to do in the future and at what stage of criminality they are. In particular, understanding the state of mind of a subject of interest – which cannot be achieved through access to metadata alone – allows investigators to make key assessments of the risk of them following through with their plans and to what timescales. This allows those investigators to take vital action to prevent crimes from taking place. That is particularly crucial in the context of counter-terrorism where, in most cases, the investigation is taking place before an attack has occurred and the primary objective of our agencies is to stop it from happening and prevent innocent people from being killed on our streets.

10. The use of end-to-end encryption by the perpetrators of terrorism and other serious crimes negates the ability of our law enforcement agencies to gain access to content in these circumstances, which creates a severe diminution in those agencies' abilities to protect the public from harm.

11. Given the importance of these powers and the impact end-to-end encryption is having on their use, there is increasing unanimity across like-minded governments and international institutions: while the use of encryption is vital, that should not come at the expense of precluding law enforcement from being able to access the content of communications where that is needed to progress their investigations and is subject to robust safeguards and oversight. In July 2019, the governments of the United Kingdom, United States, Australia, New Zealand and Canada issued a joint statement, concluding that: "tech companies should include mechanisms in the design of their encrypted products and services whereby government, acting with appropriate legal authority, can gain access to data in a readable and usable format."[2]. On 8 October 2019, the Council of the European Union adopted its conclusions on combating the sexual abuse of children, stating that: "The Council urges the industry to ensure lawful access for law enforcement and other competent authorities to digital evidence, including when encrypted or hosted on IT servers located abroad, without prohibiting or weakening encryption and in full

[2] https://www.gov.uk/government/publications/five-country-ministerial-communique/joint-meeting-of-five-country-ministerial-and-quintet-of-attorneys-general-communique-london-2019

respect of privacy and fair trial guarantees consistent with applicable law."[3]. And on 11 December 2019, the United States and European Union made this joint statement following the US, EU Justice and Home Affairs Ministerial meeting: "We also acknowledged that the use of warrant-proof encryption by terrorists and other criminals – including those who engage in online child sexual exploitation – compromises the ability of law enforcement agencies to protect victims and the public at large. At the same time, encryption is an important technical measure to ensure cybersecurity and the exercise of fundamental rights, including privacy, which requires that any access to encrypted data be via legal procedures that protect privacy and security. Within this framework, we discussed the critical importance of working towards ensuring lawful access for law enforcement and other law enforcement authorities to digital evidence, including when encrypted or hosted on servers located in another jurisdiction."[4].

Company access:

12. Regarding the ability of companies to detect and tackle illegal content themselves, the risks posed by the application of end-to-end encryption are well documented. As the open letter to Mark Zuckerberg of 4 October makes clear, it is estimated that Facebook's proposals would remove 12 million reports to the National Center for Missing and Exploited Children (NCMEC) every year. In 2018, those reports will have led to more than 2500 arrests by UK law enforcement and almost 3000 children safeguarded in the UK alone[5]. Those numbers are hard to comprehend, and it is worth pausing to reflect on them. That is almost 3000 children who could otherwise go on being abused, raped and degraded, and having their lives ruined. That is more than 2500 arrests preventing offenders from continuing to be able to go on perpetrating these disgusting crimes and targeting more and more victims. That is in only one country. That is in only one year. That is based on referrals from only one company. That is what we stand to lose.

13. The scale of this impact is even more terrifying when you consider the horrendous detail that sits behind individual cases. In 2017 content from Facebook Messenger provided to UK police as a result of Facebook's own monitoring showed that a UK based individual identified as Paul Leighton had uploaded a first-generation indecent image of a child and conducted sexualised conversations with a child. Further content from multiple Facebook Messenger accounts showed Leighton posing as a young female in order to reach out to children on Facebook Messenger, gaining their trust by using their social media information to build false relationships. The content of messages sent over Facebook Messenger showed Leighton persuading his victims to send him self-taken indecent images of themselves which were then used to blackmail the children into providing progressively more extreme content, often by threatening to flag the child's behaviour to family or friends via Facebook. This included coercing children into performing degrading acts with family pets and the rape and sexual abuse of

[3] https://data.consilium.europa.eu/doc/document/ST-12862-2019-INIT/en/pdf
[4] https://www.justice.gov/opa/pr/joint-us-eu-statement-following-us-eu-justice-and-home-affairs-ministerial-meeting-0
[5] https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg/open-letter-from-the-home-secretary-alongside-us-attorney-general-barr-secretary-of-homeland-security-acting-mcaleenan-and-australian-minister-f

siblings. Leighton, who was not previously known to the authorities for online offending, was sentenced to 27 years in jail. Without the trigger provided by Facebook's own monitoring of content this investigation would not have been instigated, multiple children would not have been safeguarded, and Leighton may have continued to draw in more young victims[6].

14. There is increasing evidence and recognition of the grave impact the implementation of end-to-end encryption can have on a company's ability to identify and tackle child sexual exploitation and abuse, including grooming and the sharing of child abuse imagery. The UK National Society for the Prevention of Cruelty to Children (NSPCC) recently reported that there are, on average, eleven reports of online child sex crimes to the police every day from Facebook's services in the UK alone. They concluded that Facebook's move to end-to-end encryption risks making them a "one stop grooming shop"[7]. In addition, the recently published Global Threat Assessment for 2019 from the WeProtect Global Alliance – an international movement supported by more than 84 nation states and non-governmental organisations dedicated to ending child sexual abuse – concluded that: "End-to-end encryption creates a risk to children as it prevents online platforms and their moderators from identifying, removing and reporting harmful content from critical parts of their own networks."

15. The risks to companies' own abilities to detect and act against terrorist material are also severe. For example, Facebook's transparency reports show that they acted against 26 million pieces of terrorist content between October 2017 and March 2019[8]. The company hasn't quantified how much of this activity would be lost if they apply end-to-end encryption as planned. But any diminution in our ability, and that of the tech industry, to identify and tackle terrorist material would of course have a very serious impact on public safety.

16. Given the severity of these impacts, we have a duty as a Government to respond. I will focus in this statement on the UK Government's legal and policy response to the first of these challenges, lawful access. That reflects the explicit emphasis of the Committee's hearing. It also reflects that it is our response to lawful access that is most frequently misunderstood and misinterpreted in the public debate and as the UK senior official responsible for that response, I see it as my duty to explain it. Notwithstanding the specific focus of the rest of this testimony, the two distinct areas of the impact of end-to-end encryption on public safety are equally important to the UK Government. And while these challenges are distinct and will require different technical solutions, it is absolutely the case that the overarching policy approach that we advocate as the UK Government – focused on detailed, technical engagement with industry about reasonable proposals, underpinned by strong and balanced principles – applies equally to both.

---

[6] https://www.bbc.co.uk/news/uk-england-tyne-41153941

[7] https://www.telegraph.co.uk/news/2019/12/05/nearly-half-online-child-abuse-reports-police-facebook-apps/

[8] https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg/open-letter-from-the-home-secretary-alongside-us-attorney-general-barr-secretary-of-homeland-security-acting-mcaleenan-and-australian-minister-f

UK response on lawful access:

17. A primary responsibility of any state is to ensure the security, safety and wellbeing of its citizens, including through upholding fundamental rights and freedoms. Tech companies have made promises to their users to protect their data, law enforcement have a legitimate need to gather data from or about individuals to tackle the most serious crimes, and citizens have the right to expect that their privacy will be protected. All these factors need to be weighted appropriately.

18. Too often, the debate on lawful access and end-to-end encryption has been described as a fight between privacy and national security, implying that you can either have one or the other. The reality is that we must look for solutions that respect both, as well as protecting cyber security and without having a detrimental impact on technological innovation. We believe that will be possible in the majority of cases. In striving to achieve this balance, we should be as transparent as we can be without having a negative impact on the operational capabilities of our law enforcement and intelligence agencies. That means being transparent about what we do and do not need, about what powers are available to our operational agencies, and in certain circumstances it may also mean being more transparent about where lawful access systems exist.

19. As a Government, our starting point in achieving this balance is to have a clear legal framework, openly scrutinised and approved by Parliament, that provides our law enforcement and intelligence agencies with the powers they need to investigate crime and defend our national security, while ensuring that data protection and privacy are at the heart of those powers and that they are subject to strong safeguards and oversight. In the UK, this is provided by the Investigatory Powers Act 2016.

20. This legislation was brought forward following three detailed independent reviews on the use of investigatory powers carried out in 2015. The first of those reviews was conducted by the former Independent Reviewer of Terrorism Legislation, David Anderson (now Lord Anderson of Ipswich KBE QC). That review, which was required in statute, examined in detail threats to the UK, capabilities required to combat those threats, safeguards to protect privacy, the challenges presented by changing technologies, as well as transparency and oversight. David Anderson's review received almost 70 written submissions from across academia, the technology sector and civil society, and was informed by evidence from the Government at the highest levels of security clearance[9]. The second review, undertaken by the Intelligence and Security Committee of the UK Parliament, considered the full range of intrusive capabilities available to the UK intelligence services and contained an unprecedented level of detail about those capabilities, the legal framework that governed their use at that time and the privacy protections

[9] "A Question of Trust: Report of the Investigatory Powers Review", David Anderson QC, Independent Reviewer of Terrorism Legislation, June 2015 (https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/)

and safeguards that applied[10]. The final review was carried out by an independent panel convened by the Royal United Services Institute, including parliamentarians, academics and former heads of each of the UK's three intelligence services. That review considered specifically the UK operational agencies' statutory powers in the face of changing technology[11]. Each of those reviews concluded that comprehensive new legislation should be taken forward on investigatory powers.

21. The then Investigatory Powers Bill responded to the three reviews, addressing the majority of their recommendations and bringing together the powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications, subjecting them to significantly enhanced safeguards.

22. Before being introduced to Parliament, the Bill was published in draft in November 2015 and subjected to very thorough pre-legislative scrutiny. That included detailed consideration by three separate parliamentary committees: a Joint Committee of both Houses of Parliament convened specifically to examine the draft Bill[12]; the Science and Technology Committee[13]; and the Intelligence and Security Committee[14]. Between them, these committees considered over 1500 pages of written evidence and took oral evidence from the Government, industry (including tech companies from the UK and US), civil liberties groups and many others.

23. The revised Bill that was introduced to Parliament in March 2016 gave effect to the vast majority of the Committees' recommendations. Alongside the Bill's introduction, the Government published a detailed response to the Committees' reviews, setting out how we had dealt with each and every one of their recommendations[15].

24. Following introduction, the Bill's parliamentary passage involved a level of scrutiny that was almost unprecedented. In total, over 1700 proposed amendments to the legislation were considered prior to Royal Assent on 29 November 2016. Those proposed amendments, many of which the Government either accepted or responded to by making substantive changes to the Bill, resulted in a better piece of law that truly reflected the will of Parliament. As the director responsible for the

[10] "Privacy and Security: A Modern and Transparent Legal Framework", Intelligence and Security Committee of Parliament, March 2015 (http://isc.independent.gov.uk/committee-reports/special-reports)
[11] "A Democratic Licence to Operate: Report of the Independent Surveillance Review", Panel of the Independent Surveillance Review, July 2015 (https://rusi.org/publication/whitehall-reports/democratic-licence-operate-report-independent-surveillance-review)
[12] "Report – Draft Investigatory Powers Bill", Joint Committee on the Draft Investigatory Powers Bill, February 2016 (https://www.parliament.uk/draft-investigatory-powers)
[13] "Report: Investigatory Powers Bill: technology issues", Science and Technology Committee (Commons), January 2016 (https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/inquiries/parliament-2015/investigatory-powers-bill-technology-issues-inquiry-launch-15-16/)
[14] "Report on draft Investigatory Powers Bill", Intelligence and Security Committee of Parliament, February 2016 (http://isc.independent.gov.uk/committee-reports/special-reports)
[15] "Investigatory Powers Bill: government response to pre-legislative scrutiny", HMG, March 2016 (https://www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents)

team that oversees that legislation, I expect to continue to have to explain the substance of its provisions and welcome that process as an important part of living in a democracy. However, it is disheartening when the Act is referred to dismissively as the "Snoopers' Charter" or portrayed as having been "nodded through" Parliament. It will be clear to anyone willing to engage substantively on this issue that this is a mischaracterisation. As David Anderson put it shortly following the Act being passed into law, the passage of the Investigatory Powers Act was an "exercise in democracy"[16].

25. The Act has radically overhauled the way in which investigatory powers are authorised and overseen. It has required that warrants for the use of the most intrusive powers be approved by the Secretary of State and an independent judge. It has also created a powerful Investigatory Powers Commissioner, currently Sir Brian Leveson, to oversee the use of these powers, supported by a well-staffed office including legal and technical experts.

26. The Act is world leading legislation and that is underlined by the conclusions of the UN Special Rapporteur on the right to privacy, Joe Cannataci, who examined in detail the Investigatory Powers Act in 2018 and stated that: "Given its history in the protection of civil liberties and the significant recent improvement in its privacy law and mechanisms, the UK can now justifiably reclaim its leadership role in Europe as well as globally"[17].

27. I will now explore how exactly the Investigatory Powers Act plays into the encryption debate. Most people understand the concept of an interception warrant. In UK law, a targeted interception warrant can be issued in relation to a particular subject where necessary and proportionate for extremely limited purposes. When served on a communications service provider, the warrant requires them to do what is reasonably practicable to intercept the target's communications and disclose them to the relevant investigating agency.

28. In practice certain companies handle very large numbers of communications meaning they may be required to give effect to interception warrants on a recurrent basis. So it is understandable that we would expect some companies to maintain specific, ongoing capabilities to enable them to give effect to warrants securely and quickly. The Investigatory Powers Act provides for this by enabling the Secretary of State to give a communications service provider a technical capability notice. The requirements that such a notice may impose are primarily about ensuring companies only collect the data authorised, deliver it to the assigned agency in a secure manner and guarantee that all aspects of this process are auditable. This concept is not new in our legal framework and broadly equivalent

[16] "The Investigatory Powers Act 2016 – an exercise in democracy", David Anderson QC, December 2016 (https://www.daqc.co.uk/2016/12/03/the-investigatory-powers-act-2016-an-exercise-in-democracy/)

[17] "End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion of his Mission to the United Kingdom of Great Britain and Northern Ireland" Joe Cannataci, United Nations Special Rapporteur on the right to privacy, June 2018 (https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E)

notices could be given under our previous legislation, the Regulation of Investigatory Powers Act 2000[18].

29. Technical capability notices can also detail the format we would want data in, which is the crux of the encryption debate. The notice itself is not a tool to compel the provider to release data, a duly authorised warrant is still required each time data is requested. That means technical capability notices can't be used to require companies to provide unfettered access to the communications of their users. However, they can provide a legal basis to ask a company to establish a lawful access mechanism to encrypted communications.

30. Our legal framework sets out two ways in which technical capability notices might require a communications service provider to help the Government deal with the encryption they apply to data: to maintain the capability either to remove encryption or to provide data or communications in an intelligible form. That distinction is set out in our legislation itself and is important because the means by which lawful access could be achieved will change on a case by case basis, which is fundamental to our policy approach and to our principles. I will return to questions about what it may or may not be reasonable to expect companies to do in this area but we accept it will not always be reasonable, or desirable, to expect companies to provide for lawful access by maintaining the capability to remove encryption. We would invariably seek to avoid requiring a company to implement a lawful access solution that fundamentally changed the trust relationship between a service provider and its users. That will often mean finding ways to provide access to communications in an intelligible format without removing cryptography. It could also mean requiring an operator to maintain the capability to provide access to content in certain circumstances but not in others.

31. I have already highlighted the importance of having a legal framework that ensures the investigatory powers we provide to our law enforcement and intelligence agencies are subject to strong safeguards and oversight. It is worth summarising what that looks like specifically in relation to technical capability notices.

32. Like warrants issued under the Act, technical capability notices must be approved by an independent judge working with the Investigatory Powers Commissioner before they can be given. When deciding whether to approve a notice, those judges have the benefit of input from a group of independent technical experts sitting on the Technology Advisory Panel, which was established under the Act and reports to the Commissioner. Like warrants, notices may not be given unless they are necessary and proportionate. In relation to maintaining the capability to remove encryption or provide communications or data in an intelligible form, any such obligation must be reasonably practicable for the operator to comply with. That is a key legal test and recognises that it will not be possible to achieve 100% access 100% of the time, even where there is a legitimate need.

[18] Prior to being repealed with the commencement of relevant provisions in the Investigatory Powers Act 2016, section 12 of the Regulation of Investigatory Powers Act 2000 provided that the Secretary of State could give a notice requiring a person providing public telecommunications services to maintain interception capabilities.

33. Prior to deciding to give a notice to an operator, the Secretary of State must consult them. The Act also requires that the Secretary of State considers a number of other matters before deciding to give a notice, including the technical feasibility and likely cost of complying with it, as well as the public interest in the security and integrity of telecommunications systems.

34. Further safeguards apply after a technical capability notice has been given to an operator, including the ability for them to seek a review of it by the Secretary of State. Before the Secretary of State decides the outcome of the review, they must consult a Judicial Commissioner in relation to the necessity and proportionality of the notice and an independent Technical Advisory Board in relation to the technical requirements and financial consequences of it (despite the similar name, the Technical Advisory Board is distinct from the Technology Advisory Panel and must include both individuals representing investigating agencies and those representing industry). If the outcome of the review is to maintain the effect of the notice, that decision must be approved by the Investigatory Powers Commissioner.

35. That is a long and comprehensive set of safeguards and oversight. However, as mentioned above, a strong legal framework is just the starting point in achieving the appropriate balance in our policy position on lawful access. Legislation can't provide all the answers. The Investigatory Powers Act is technology neutral, as far as possible, to avoid the need for amendments as technology changes over time. That also provides the necessary space for individual operators to be able to identify solutions on a case by case basis and for UK law enforcement and intelligence agencies to adapt their investigative tradecraft as technology changes.

36. We rely on important legal tests like necessity and proportionality or, in the context of lawful access, reasonable practicability, to determine what is permissible. While those are entirely appropriate tests to include in our legislative framework, we must be prepared to explain what we mean by them. As set out in the Lawfare article, the technical details are what really count and the potential for lawful access solutions to be established will depend on how individual services are designed.

37. Nevertheless, I believe the Government has a responsibility to set out in as much detail as we can what we are trying to achieve and what we expect from our engagement with industry on this issue. That is why our principles are so important. The principles set out in the Lawfare blog are replicated below and all of them are referenced in what I have already said. That is key because they are so fundamental to everything that we say on this issue as the UK Government.

    1) Privacy and security protections are critical to public confidence. Therefore, we will only seek exceptional access to data where there's a legitimate need, that access is the least intrusive way of proceeding and there is appropriate legal authorisation.
    2) Investigative tradecraft has to evolve with technology.
    3) Even when we have a legitimate need, we can't expect 100 percent access 100 percent of the time.

4) Targeted exceptional access capabilities should not give governments unfettered access to communications.
5) Any exceptional access solution should not fundamentally change the trust relationship between a service provider and its users.
6) Transparency is essential.

38. I will now explain more about how these principles fit into our approach. The first thing to note is that they do not just apply to discussions about technical capability notices or legal compulsion and the publication of the principles certainly wasn't a pretence for the giving of a technical capability notice. Hopefully it is clear from the very comprehensive safeguards that would be involved in that process that their publication could never serve that function. The Government wants to work with a range of providers in relation to achieving lawful access in a range of contexts and the principles are deliberately silent on the mechanism through which that could be achieved. If we were working with a company to gain access voluntarily, giving them a technical capability notice, or just engaging them on an exploratory basis, we would expect to be held to account against the principles we have set ourselves.

39. Another key point about the principles, and our overarching policy approach, is the importance of taking a coordinated view. The Lawfare blog refers to the fact that the principles were developed with colleagues across Government departments and agencies, representing many different policy and operational interests. As a Government, we cannot hope to achieve the required balance if we simply make this an issue led by departments and agencies that are focused on national security and law enforcement. There is a need to involve departments focused on promoting technical innovation, privacy, freedom of expression and cyber security. In the UK that means everything we do on this issue is done alongside the Department for Digital, Culture, Media and Sport, the Foreign and Commonwealth Office, the Cabinet Office and the National Cyber Security Centre, as well as the intelligence agencies and law enforcement.

40. All those departments were closely involved in the development of our principles. This means we can say with a united voice that we believe we are taking a balanced and informed approach as the UK Government and that this approach respects citizens' cyber security and privacy. That doesn't mean our principles are immovable or set in stone. As stated, the purpose of publishing them in the first place was to start a conversation and we want to continue it. We are open to ideas of how to adapt our approach and we expect questions to keep being asked of us on this issue.

41. One question we face repeatedly is whether the creation of a lawful access mechanism amounts to the insertion of so-called "backdoors" into tech companies' services, enabling unfettered access to communications or an opening for hackers and other malicious actors to exploit. It will be clear to anyone who has considered in detail our legislation and our principles that nothing we have ever called for, or could call for under our law, could fairly be characterised as a "backdoor". This is an ill-defined and unhelpful analogy and I believe it is often used to detract from participating in a sensible debate between technical experts.

42. If we are to foster such a debate, we must recognise that we do not deal with absolutes in cyber security. I have already said that we would not ask to implement a lawful access solution that fundamentally changed the trust relationship between a service provider and its users. That reflects that no real system is perfectly secure and companies – including those running end-to-end encrypted services – make conscious choices themselves to increase the usability of their systems that could reduce the security and privacy of their users. That doesn't mean those services cannot be trusted or are somehow insecure. It simply reflects that they are designed for real people and must include features that reflect that, such as ensuring an individual's data or account can be recovered when they forget their password, lose their phone, buy a new device, and so on.

43. We do not subscribe to the view that every extra line of code that is added to a service is a vulnerability waiting to be exploited. That doesn't have to be true for any features, relating to lawful access or otherwise. While the debate on this issue often portrays cryptography as an academic, inviolable construct, what we are really talking about in the context of end-to-end encryption is the risk profile of a software change. Indeed, using the term vulnerability in the context of lawful access is itself misleading. We are not talking about companies introducing vulnerabilities to their services, we are talking about them introducing additional functionality. As with the introduction of any new function, that would need to be underpinned by a detailed design, implementation and management process to industry good practice standards that respected the importance of cyber security and the protection of users' data and privacy. That is not something that could reasonably be equated to a "backdoor".

44. Many companies strike a balance now without creating undue risks to the security of users' data. That includes some of the largest tech companies in the world, running some of the largest and most popular messaging services. I am sure that those companies would strongly – and rightly – reject the notion that their services are somehow a hotbed for hackers or provide so-called "backdoors", simply on the basis that their services aren't currently designed with end-to-end encryption that precludes law enforcement access where necessary and proportionate.

45. Another common question we face is what countries the tech companies should choose to work with and whether the creation of a lawful access mechanism for one government will theoretically provide access to other governments too?

46. Gaining lawful access to the communications of individuals of intelligence interest is a transnational challenge. The UK Government is not the only democratic government that has a legitimate need to provide such access to their investigating agencies. We don't believe it is automatically a problem that the result of developing a lawful access mechanism for one country might be that other governments, that have a functioning democracy and respect the rule of law, can also enhance their lawful access to data of investigative value. That creates challenges though because different countries apply varying levels of safeguards and oversight and we don't believe service providers should decide, or be forced to decide, from which governments they should accept lawful orders to access data.

47. This is a difficult issue but one where we believe progress can be made. On 3 October 2019, the UK Government signed a world first reciprocal bilateral data access Agreement with the United States, pursuant to the Clarifying Lawful Overseas Use of Data Act 2018 (CLOUD Act). The Agreement is neutral on the specific issue of encryption but removes legal barriers to service providers in each country responding directly to requests for data from the other country's agencies, as long as both countries and each request meet certain criteria. The Agreement is based on respecting the rule of law and international universal human rights and having clear statutory governance of lawful access regimes, including effective independent oversight. Orders must concern a specific target, relating to the prevention, detection, investigation or prosecution of serious crime, justified on the basis of credible facts which must be subject to review by a judge or another similarly independent authority.

48. We believe the Agreement provides an international model for the future. That model allows democratic governments to recognise and facilitate others' legitimate interest in accessing data controlled within their jurisdiction. It does that without creating indiscriminate access for countries which don't share our own high standards of proportionality, democratic legitimacy and accountability, underpinned by independent oversight. We envisage that the prospect of such an Agreement will provide a key way of incentivising countries to improve their own standards.

49. These approaches provide a model for like-minded, democratic countries that respect the rule of law and human rights. However, we also need to answer questions about what impact the creation of a lawful access mechanism might have in relation to authoritarian states or oppressive regimes. In particular, we often see arguments that if tech companies do not apply end-to-end encryption in such a way that precludes lawful access for anybody then there would automatically be an increased risk of authoritarian states being able to break into individuals' messages.

50. Strong encryption serves a vital purpose in repressive states to protect journalists, human rights defenders and other vulnerable people. However, arguments about this are often conflated and it is helpful to break them down. It is important to remember that the technical difference we are talking about is whether the provider of a service retains a technical capability to access the content of communications that are already encrypted over that service. It is not the difference between messages being end-to-end encrypted or not encrypted at all. That is key for understanding properly the potential impact for an oppressive regime in terms of its own, independent ability to access the content of those messages.

51. For example, if an oppressive state was to try and intercept the communications of one of its citizens through their broadband line or mobile network, encryption applied by a tech company operating from another jurisdiction – be that from the US or elsewhere – would prevent the content of messages being readable. That would be the case whether that company could access those messages itself, or

whether end-to-end encryption had been applied in such a way that they could not.

52. Alternatively, were that oppressive regime able to hack directly into the device of one of its citizens, then they are likely to be able to read the content of that person's messages at the endpoint – in the same way the user can – irrespective of the type of encryption being applied to those messages when they are in transit. Whether a message is end-to-end encrypted or not wouldn't make any difference in that scenario.

53. There is a more fundamental scenario in which people hypothesise on the impact were an oppressive state able to hack directly into the central systems and servers of a tech company based in another jurisdiction. Were they able to do so then, theoretically at least, they would be able to read the content of users' messages that would not be available were they end-to-end encrypted. However, it is important to recognise that were this sort of access achieved – which would go to the very core of a company's ability to protect itself from cyber-attacks – then it would have extremely far reaching consequences. With a level of access that fundamental, it is highly likely that a hostile actor would also be able to have other profound effects on the company's services including, and extending beyond, impacting directly on what information could be accessed through an end-to-end encrypted service. That could include impacting identity systems, changing the source code for the client app, abusing the vast sets of data tech companies collect for advertising purposes, and so on.

54. The implementation of end-to-end encryption of course doesn't change materially the level of technical risk or protection from a prospective offensive state being able to gain that sort of access to a company's systems in the first place. What does make a difference are the security protections that a company puts in place to defend its core infrastructure and users' data – including messaging content but also other forms of intrusive personal information such as metadata, location data, financial information, and so on. And as I have already said, we are talking about some of the largest tech companies in the world who currently deploy some of the most sophisticated security protections. That enables them to protect the content of their users' messages from malicious actors, without having to resort to putting all of that content out of their own reach, in all circumstances.

55. The question then again becomes what countries a tech company chooses to work with, including whether they would respond to direct requests from oppressive regimes for content or other data running over their services. The answer to that question takes us straight back to the development of international agreements under the CLOUD Act because authoritarian regimes would never be able to demonstrate the standards required to secure such an Agreement.

56. International agreements provide a powerful means of raising and aligning standards and preventing nation states that cannot meet those standards from demonstrating that they should be provided lawful access to data. Nonetheless, even among countries that would qualify for such an agreement, different nations will continue to have different legal bases underpinning their requirement for the

development of lawful access solutions. Other democratic countries may have provisions in law that look similar to our technical capability notices, however, they will of course not be the same. However, one thing that governments can align is their overarching approach, which brings us straight back to the principles. Like-minded governments should be able to agree what is and isn't needed, and what is and isn't possible, in the pursuit of lawful access mechanisms. The question then becomes less about companies responding to multiple requirements from individual governments and more about responding to a single, global requirement to ensure criminals and other dangerous individuals can be investigated effectively where appropriate safeguards are in place.

57. In August 2018, the UK signed up to a joint statement alongside the governments of the US, Canada, Australia and New Zealand on access to evidence and encryption, which committed us all to supporting strong encryption while seeking access to data. That statement was a starting point, urging signatories to pursue the best way to implement it within their jurisdictions. As the Lawfare article makes clear, that is where details matter, which is why we brought forward the UK's own principles last year and why we want to continue the debate.

58. Our principles, underpinned by our legislation, set out a framework for engaging industry on lawful access that strikes the right balance between our responsibilities and those of the tech companies. We believe such engagement is likely to identify opportunities that, without compromising the wider safety and security of systems for lawful users, can provide ways to gain specific, targeted and lawful access to information about what terrorists, child sex abusers and the perpetrators of other serious crimes are doing online.

59. Addressing the severe public safety threats that we face because of the use of end-to-end encryption is a matter of the utmost priority for the UK Government. It is vital that international governments and the tech industry work together to find technical solutions that balance effective law enforcement, effective cyber security and effective privacy. If we do not get this right then the impact on the safety of our citizens, and our children, will be stark.