Independent Reviewer of Terrorism Legislation
David Anderson QC
Brick Court Chambers
7-8 Essex Street
London
WC2R 3LD

Evidence for Investigatory Powers Review
Submitted by Access

Table of Contents

Introduction

Access welcomes the opportunity to submit evidence to the Investigatory Powers Review, and to inform Parliament's continuing work on this crucial area of law and regulation.

In our submission, we recommend that Parliament consider its laws and policies related to communications surveillance, specifically in regards to the impacts on fundamental human rights of internet and telecommunications users. The International Principles on the Application of Human Rights to Communications Surveillance ("the Principles"),[1] which provide a framework for assessing states' human rights duties and obligations when conducting surveillance, are particularly instructive in this regard. The Principles, which Access helped to draft, have been endorsed by more than 400 civil society organizations around the world. The landmark 2014 report by the UN High

[1] https://en.necessaryandproportionate.org/text.

Commissioner of Human Rights Navi Pillay acknowledged that the Principles can serve as interpretive guidance of Article 17 of the International Covenant on Civil and Political Rights.[2]

Long legacies of the exercise of free expression, privacy, and other civil and political rights in the UK should continue into the digital age. Fortuitously, digital rights protections also benefit innovation and the information economy, and will ensure that international businesses and users see the UK as a safe, secure place to conduct online activity and commerce.

Diverse stakeholders have labored to strengthen global standards on transparency and privacy, and now seek more uniform implementation in domestic law to protect human rights and increase accountability worldwide. The UK can play strong role in this effort by reforming its surveillance legislation to protect rights online as they are offline, for its citizens and users around the world. To achieve these goals, we urge greater transparency on the government's surveillance activities; critical review of data retention mandates for consistency with international law and norms; and principled vigilance on any government interference with cryptographic standards.

1) Increasing Trust and Certainty

One year after the release of the International Principles on the Application of Human Rights to Government Surveillance, secrecy continues in the UK and elsewhere through overbroad laws, judicial and legislative gag orders, and threats of retaliation for disclosures. Silence on the scope and scale of government surveillance leaves users in the dark, harms the reputations of private companies, and destroys trust and certainty in the information economy. In the UK, especially, secret courts and policies restricting the reporting and disclosures deter from efforts to inform citizens on the extent of surveillance online.

States and service providers both have rights and responsibilities regarding transparency on communications surveillance. Governments should pursue both the active role of keeping users informed of the processing and transfer of their personal data, as well as the more passive role in recognizing the right of providers to do the same.

[2] OHCHR, *The Right to Privacy in the Digital Age*, http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

Moreover, providers often say that "transparency is the government's responsibility." On surveillance, they maintain, governments are better positioned to disclose surveillance practices than the businesses processing their requests. For their part, governments must loosen restrictions and disclose data on their own activities, including in national security.

Transparency Reports, beyond the numbers

At their best, "transparency reports" can reveal the scope and scale of surveillance online. Generally, they include aggregate statistics of requests that governments issue for user data, giving details like the type of request, why it was issued, and whether the recipient complied. They're one of the proactive ways that companies, governments -- really any entity dealing with user data -- can directly inform users about risks to their communications and other activities online.

Governments have made some progress on transparency. Earlier this year, the U.S. government reached a settlement[3] with major internet platforms allowing them to release aggregate data on certain national security requests. Companies have upheld their end of the bargain, as more and more firms adhere to the government's strict guidelines and report national security requests for the first time. Yet companies eager to regain the trust of users still push for more transparency: the U.S. government imposed a delay on acknowledging Foreign Intelligence Surveillance Court (FISC) orders, and only allows statistical reporting in bands of several hundred.[4] Elsewhere, various governments and departments have succeeded in engaging the public with open data policies. In Hong Kong, government statistics come alive through the skillful visualization and helpful explanations in the Hong Kong Transparency Report.[5]

To date, however, most States have lagged far behind of internet and telecommunication providers when it comes to reporting on their surveillance activity. Ironically, it took a private service provider, UK-based Vodafone, to reveal the legal and operational context of government surveillance -- and just how much we don't know.[6] Out of 29 countries where Vodafone does business, governments in 8 either bar disclosure of surveillance requests, or were, at the time of the report, too unstable to even approach with the question, according to the company. In 10 countries,

---

[3] WSJ, *Government Reaches Deal With Tech Firms on Data Requests*, http://online.wsj.com/news/articles/SB10001424052702303277704579347130452335684.

[4] Twitter, *Fighting for more transparency*, https://blog.twitter.com/2014/fighting-for-more-transparency

[5] Hong Kong Transparency Report, http://transparency.jmsc.hku.hk.

[6] Vodafone, *Law Enforcement Disclosure Report*, http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf.

Vodafone's report marked the first time any entity, either provider or government, had published surveillance data. Another handful of states enjoy direct access to the company's networks, leaving the provider, and users, no idea of the extent of surveillance and the corresponding interference with user rights taking place.

In the U.S., the bulk of communications metadata collected still falls into a legal black hole. The DOJ settlement did not allow reporting on the number of customer accounts affected by FISA Section 215 orders, which require telecom providers to deliver metadata of daily call records, affecting millions of users.[7] The U.S. intelligence directorate's own transparency report similarly lacked rigor and clarity[8] on the scale and scope of government surveillance, falling short of the granularity that the "We Need to Know Coalition" -- a multistakeholder group including companies like Google and Microsoft, NGOs including Access, CDT, and the ACLU, and trade associations -- has identified as necessary.[9]

UK Transparency

The UK has shown some foresight on transparency, creating the Interception of Communications Commissioner's Office with the passage of RIPA in 2000. This Office publishes statistical information on lawful interception and communications data demands issued by agencies and authorities. While its 2013 report[10] provided greater detail than previous releases, the Commissioner's reports have been broadly criticized as lacking in scrutiny, failing to break down surveillance requests into granular categories, and being critically circumscribed in scope.

In the UK, according to Vodafone,

> Section 19 of the Regulation of Investigatory Powers Act 2000 prohibits disclosing the existence of any lawful interception warrant and the existence of any requirement to provide assistance in relation to a warrant. This duty of secrecy extends to all matters relating to warranted lawful interception. Data relating to lawful interception warrants cannot be published. Accordingly, to

[7] https://www.techdirt.com/articles/20140127/17253826014/feds-reach-settlement-with-internet-companies-allowing-them-to-report-not-nearly-enough-details-surveillance-efforts.shtml
[8] https://www.accessnow.org/blog/2014/06/27/us-intelligence-report-misses-opportunity-for-openness
[9] Access, *We Need to Know: Companies, Civil Society Call for Transparency on Surveillance*, https://www.accessnow.org/blog/2013/07/18/tech-companies-and-civil-society-join-call-on-the-us-government-to-issue-tr.
[10] IOCCO, *Annual Report of the Interception of Communications Commissioner* (2013), http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf.

> publish aggregate statistics would be to disclose the existence of one or more lawful interception warrants.[11]

Of particular interest to foreign users, the Commissioner cannot report on the number of certificates and warrants issued under Section 8(4) of RIPA, which allows for the interception of the content of communications via a certified warrant.[12] A Section 8(4) warrant "does not have to name or describe one person as the interception subject or a single set of premises as the target of the interception,"[13] according to the Commissioner, which allows its use for mass surveillance purposes. The Section 8(4) warrants "are restricted to the interception of external communications … sent or received outside of the British Islands."[14] In other words, the law targets foreign communications, directly implicating the human rights to privacy and free expression of users around the world.

Additionally, any acknowledgement of UK programs that allow police or intelligence services direct access to networks, or instances thereof, are missing from the Commissioner's reports. For instance, GCHQ conducts mass surveillance via satellites and fibre-optic undersea cables, scooping up huge volumes of data from communications between innocent people.[15] And Vodafone found that Section 5 of the Intelligence Services Act 1994 ("ISA") could grant powers "broad enough to permit government direct access to Vodafone's network by the Security Services in some instances."[16] Neither of these powers are detailed by the Commissioner.

Two-way accountability

Transparency is the first step toward accountability on UK surveillance activities, which impact millions of individuals on a daily basis. Recipients of lawful intercept warrants should be able to acknowledge and report them. As transparency reporting by businesses fast becomes a global business standard, the international community will

---

[11] Vodafone, *Law Enforcement Disclosure Report*, http://www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf, at pg. 77.
[12] See Statewatch, *Analysis*, at http://cryptome.org/2014/05/gchq-lawful-world-spy.pdf.
[13] *See supra* note 8, at 8.
[14] *Id*.
[15] Guardian, *Mastering the Internet: How GCHQ Set Out to Spy on the World Wide Web*, http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet; Guardian, *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
[16] Under this law, "the Secretary of State may, on an application made by the Security Service, the Intelligence Services or GCHQ, issue a warrant in respect of any property so specified or in respect of wireless telegraphy." *See supra* note 6, at 86.

continue to demand greater trust and certainty in UK firms as a prerequisite to trade and transfer of data across borders.[17]

For its part, the Interception of Communications Commissioner should be greatly empowered to count and question the government's wide ranging surveillance activities, with statistics broken down by agency and accounting for surveillance of foreigners.

Where both companies and governments issue transparency reports, users benefit most: two-way accountability will increase as the reports converge toward uniform standards on counting and reporting individual requests. The checks and balances these reports can provide on statistics and context help to ensure the UK public -- and foreign users -- are adequately informed about communications surveillance, and able to participate in robust debate on its proper limits.

Surveillance courts and transparent law

Secret law and secret courts do not yield legitimacy or accountability. Access supports massive changes to the U.S. Foreign Intelligence Surveillance Court (FISC), and similar calls to reform the UK's Investigatory Powers Tribunal (IPT), as both forums lack the open and adversarial processes necessary to produce legitimate law or accountable practices in accordance with international human rights standards.[18]

On the U.S. side, the publication of some court opinions has provided valuable information on the extent of government surveillance -- and bolstered calls to make public many more opinions. The opinions revealed that a "special advocate" is needed to counter the government's arguments.[19] The U.S. President's Review Group on Intelligence and Communications Technologies suggested the special advocate be summoned on the discretion of the FISC judge, ostensibly for cases with novel questions or with wide-reaching impact.[20] Under the Review Group's recommendations, the special advocate would also receive docket information and be allowed to join the proceedings on their own initiative (without an invitation).

---

[17] To this end, Access and our partners have called providers like BT, who do not currently issue transparency reports, to begin doing so immediately. See https://www.accessnow.org/blog/2014/07/18/bt-no-transparency-report-in-the-foreseeable-future.

[18] *Don't Spy on Us: Reforming Surveillance in the UK*, https://www.openrightsgroup.org/assets/files/pdfs/reports/DSOU_Reforming_surveillance.pdf

[19] See Access, *Structural Changes to Surveillance Court Offer Hope for New Protections for Non-US Users*, https://www.accessnow.org/blog/2014/01/24/structural-changes-to-surveillance-court-offer-hope-for-new-protections-for, for a delineation of the powers this advocate should carry.

[20] http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf%20

The UK IPT similarly must undergo reform of its procedures and judgments. Rather than increasing the number of secret hearings, as has been proposed,[21] the IPT should empower the subjects of surveillance with notice of pending complaints, and constant representation by the court's special advocates. The court should publish its opinions, open decisions to judicial review and appeals, and proceed with the presumption that cases be held in open forums, by default.

These U.S. and UK surveillance court reforms are necessary, but far from sufficient, to reform the perception of rubber-stamp surveillance authorities that routinely fail to provide effective remedy for users at risk.

2) Data Retention: Disproportionate, Unnecessary, and Costly

Blanket data retention increases risks and costs to companies and users, while turning all citizens into suspects. We submit evidence that the U.S. government has sent mixed signals on the utility of data retention for surveillance purposes, while domestic and international jurists have not been so forgiving.

U.S. law and regulations

Lacking a mandatory data retention law in the U.S.,[22] the NSA enforces de facto data retention of U.S. telephony data by holding onto the call detail records (CDRs) it bulk collects from telcos under requests made pursuant to Section 215 of the USA Patriot Act. There are some limits to this retention: since at least 2006, the Foreign Intelligence Surveillance Court (FISC) has told the NSA to destroy these records after five years.[23] In January 2014, this requirement was codified in FISC Judge Reggie Walton's Primary

[21] Guardian, *Ken Clarke Warned Plan to Curb Open Justice is Flawed*, http://www.theguardian.com/politics/2012/jan/08/ken-clarke-curb-open-justice-flawed.

[22] An FCC regulation adopted in 1986, 47 CFR 42.6 (http://www.law.cornell.edu/cfr/text/47/42.6), does require telephone companies to retain toll call billing records for eighteen months. This scope of the regulation includes toll call subscriber and call metadata, defined as "the name, address, and telephone number of the caller, telephone number called, date, time and length of the call." Yet this does not include many types of data transmission and users of contract phone plans.

[23] *In Re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, BR 06-08 (FISA Ct. 2014) , http://www.dni.gov/files/documents/11714/FISC%20Order,%20BR%2006-08.pdf.

Order as one of several safeguards, or "minimization procedures."[24] Incredibly, the NSA fought even this modest restriction, but lost in court last March.[25]

In his ruling against the NSA's motion to extend retention periods, Judge Walton found that extending the time limit on data retention under Section 215 of the USA Patriot Act "would further infringe on the privacy interests of United States persons."[26] The judgment noted that data retention "increases the risk that information about United States persons may be improperly used or disseminated," especially considering that "the great majority of these individuals have never been the subject of investigation" for intelligence purposes. Data retention lobs a hugely disproportionate impact onto unsuspecting citizens.

Even U.S. intelligence authorities have dithered on data retention's necessity and utility. In 2006, the Department of Justice did not press the FCC to extend the retention period established twenty years earlier.[27] The NSA terminated its email metadata program in 2011.[28] And recently, both the Attorney General and the Director of National Intelligence conceded that the intelligence community does not need a data retention mandate. They argued that the current version of the USA FREEDOM Act, a surveillance reform bill lacking data retention requirements, "will accommodate operational needs while providing appropriate privacy protections."[29]

CJEU ruling and UK law

The spring 2014 ruling by the Court of Justice of the EU ("CJEU") also puts into question the lawfulness of blanket data retention in general.

---

[24] DNI, *Foreign Intelligence Surveillance Court Approves Government's Application to Renew Telephony Metadata Program*, http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/994-foreign-intelligence-surveillance-court-approves-government%E2%80%99s-application-to-renew-telephony-metadata-program.

[25] TechDirt, *DOJ Asks To Hang Onto Bulk Collections Longer, Citing Need To 'Preserve' Evidence It Has No Intention Of Presenting In Court*, https://www.techdirt.com/articles/20140227/08464126374/doj-asks-to-hang-onto-bulk-collections-longer-citing-need-to-preserve-evidence-it-has-no-intention-presenting-court.shtml.

[26] *In Re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, BR-1401 (FISA Ct. 2014), http://www.emptywheel.net/wp-content/uploads/2014/03/14-01_Opinion.pdf.

[27] EmptyWheel, *The White Paper's Selective Forgetting on FCC Phone Record Retention History*, http://www.emptywheel.net/2013/08/11/the-white-papers-selective-forgetting-on-fcc-phone-record-retention-history.

[28] Guardian, *NSA Collected US Email Records in Bulk for More than Two Years Under Obama*, http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama

[29] Letter from Eric Holder, Attorney General, and James Clapper, Dir. Nat'l Intelligence, to Patrick Leahy, Sen. (Sept. 2, 2014), http://images.politico.com/global/2014/09/04/clapperholderleahyltr.pdf.

On April 8, 2014, the Grand Chamber of the European Court of Justice ("CJEU") invalidated the EU Data Retention Directive, holding that it exceeded the bounds of the EU Charter, specifically in regard to the principle of proportionality as to the Directive's interference with the rights to privacy and data protection as set out in Articles 7 and 8.[30] Adopted by the European Union in 2006, the Data Retention Directive mandated that all telecommunications data - including mobile and landline phones, fax, and email - are to be indiscriminately collected and retained by providers for a minimum period of six months, and up to two years.[31]

To implement the Directive, the UK passed Regulations in 2009 requiring that communications data "generated or processed in connection with the provision of publicly available electronic communications services or public communications networks" be retained for a period of twelve months.[32] The invalidation of the Directive had the substantive impact of nullifying the UK Regulations and similar laws in other EU member states.[33] Despite this, the Minister of State for Immigration at the Home Office explained in May that it was of the view that "the UK Data Retention Regulations … remain in force."[34]

The CJEU ruling is decisive, highlighting the need for, at the very least, greater public debate on mandatory data retention and mass surveillance, given its adverse, unnecessary, and disproportionate impacts on fundamental rights. Yet on July 10, 2014, three months after the Directive was invalidated, the Data Retention and Investigatory Powers Act (DRIP)[35] was introduced in the UK Parliament as emergency legislation. The bill's proponents did not leave adequate time for democratic processes to take hold and shape the proposed rules. Alarmingly, the DRIP was considered under "emergency" or "fast track" procedures, which greatly diminish the public involvement and the time available for debate or consideration of alternative proposals. Instead of using

---

30 http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=150642&occ=first&dir=&cid=314051;%20http://europeanlawblog.eu/?p=2289

31 Access, *A Closer Look at EU Court's Ruling and What it Means for the Future of Data Retention in Europe*, https://www.accessnow.org/blog/2014/04/11/a-closer-look-at-eu-courts-ruling-and-what-it-means-for-the-future-of-data.

32 http://www.legislation.gov.uk/uksi/2009/859/pdfs/uksi_20090859_en.pdf

33 http://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/07/Briefing-on-the-Data-Retention-and-Investigatory-Powers-Bill.pdf

34 http://www.theyworkforyou.com/wrans/?id=2014-06-16c.199250.h&s=%28%22we+consider+that%22%29+speaker%3A11640#g199250.r0

35 https://www.gov.uk/government/publications/the-data-retention-and-investigatory-powers-bill

established process,[36] the UK Government bypassed established procedures in order to not only retain its previous authority, but to greatly expand the UK surveillance state.

By its terms, the DRIP not only re-enacts the previous Regulation, without attempting to conform to the CJEU judgment, but also grants significant new authority to "extend the territorial scope of the broad interception and communications acquisition powers under the [Regulation of Investigatory Powers Act 2000 ("RIPA")]." In practice, this will open up companies to increased obligations to retain and share data with the UK government and impede on the rights of users around the world.

In the wake of the CJEU ruling, Finland[37] and Luxembourg[38] have already announced that their national laws on data retention would be reviewed. The DRIP runs contrary to the CJEU's April judgment as well as international law and established human rights principles. In line with the Charter of Fundamental Rights of the EU, any restrictions on fundamental rights are to be subject to the principle of necessity and proportionality.[39] All surveillance programs and authorities should be demonstrably necessary, proportionate, and transparent, and "data retention or collection should never be required of service providers."[40]

High costs

Along with creating lucrative targets for malicious actors,[41] data retention mandates pose significant costs. Telecom executives have voiced concerns over standardizing their datasets to match government needs.[42] Datasets would have to be held well beyond their business purpose,[43] creating significant liability risks and negative externalities: a company's international reputation would suffer for its association with

---

36 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/328408/Guide_to_Making_Legislation_July_2014.pdf

37 http://www.helsinkitimes.fi/finland/finland-news/domestic/10120-finland-must-revise-its-data-protection-laws.html

38 http://www.gouvernement.lu/3641093/08-cjue

39 http://www.europarl.europa.eu/charter/pdf/text_en.pdf

40 https://en.necessaryandproportionate.org/text

41 Nigel Brew, *Telecommunications Data Retention—An Overview*, PARLIAMENT OF AUSTL. DEP'T OF PARLIAMENTARY SERV. (Oct. 24, 2012), http://parlinfo.aph.gov.au/parlInfo/download/library/prspub/1998792/upload_binary/1998792.pdf.

42 Marcy Gordon & Martha Mendoza, *AT&T, Verizon And Sprint Push Back Against The NSA, Too*, THE HUFF. POST (Mar. 3, 2014), http://www.huffingtonpost.com/2014/03/03/att-verizon-sprint-nsa_n_4891533.html

43 *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the Subcomm. on Crime, Terrorism and Homeland Security of the Comm. on the Judiciary*, 112th Cong. (2011) (statement of Kate Dean, U.S. Internet Serv. Provider Assoc.).

domestic surveillance regimes,[44] while its energy-wasting datacenters contribute to environmental harms.[45] Ultimately, these costs are passed on to users, hampering economic growth and innovation while reducing the global competitiveness of domestic platforms and networks.

Data retention causes adverse impacts on human rights and economic innovation, while increasing data insecurity. The UK must repeal its mandates, and allow companies to minimize data retention. After all, "Data destroyed cannot be misused."[46]

3) Benefits of Strong Cryptography

Access believes the Independent Reviewer should take this opportunity to study the participation of UK government authorities in the creation, maintenance, and dissemination of cryptographic standards and tools.

The "Integrity" Principle of the International Principles on the Application of Human Rights to Communications Surveillance offers guidance:

> In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems… .[47]

Any interference with general-use encryption standards not intended solely to correct vulnerabilities or otherwise increase the strength thereof is a facial violation of the Integrity Principle. Similarly, any failure to disclose known vulnerabilities in algorithms to be immediately patched is likewise a violation.

Though common now, this type of interference by governments did not always occur. Previously, a nation's enemies communicated in secret codes that only they knew, and that only they used — you might say it was an early example of proprietary software. So when states attempted to crack one another's communications, they used their own

---

[44] *Foreign Intelligence Surveillance Act (FISA) Reforms: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. (2014) (statement of Michael Woods, Vice President and Assoc. Gen. Counsel, Verizon Commc'ns).

[45] James Glans, *Power, Pollution, and the Internet*, N.Y. TIMES (Sept. 22, 2012), http://www.nytimes.com/2012/09/23/technology/data-centers-waste-vast-amounts-of-energy-belying-industry-image.html

[46] James Plummer, *Data Retention: Costly Outsourced Surveillance,* CATO INST. (Jan. 22, 2007), http://www.cato.org/publications/techknowledge/data-retention-costly-outsourced-surveillance.

[47] https://necessaryandproportionate.org/

cryptographic experts who worked to crack the code of their enemies, but did not interfere with communications of the general public.

However, today, encrypted digital communications are typically built upon the same open protocols, whether they are sent by an intelligence agency, a major corporation, or an ordinary user. Vulnerabilities in the security of one of these standards exposes all other stakeholders using the same protocol. In this way, weaknesses in encryption algorithms are akin to "back doors" into software, programs, and databases. The problem is, even if you trust without reservation the entity building that back door for its own use, these doors are also exploitable by other actors, be it overreaching governments, authoritarian regimes, or unaffiliated bad actors.

Encryption algorithms form the foundation of a secure internet, which in turn is the basis for personal communications and social networking, e-commerce and banking, news consumption, academic research, and just about every other major use of the internet. It is therefore important to make sure that they are as strong and secure as possible.

The UK should ensure that there is separation between entities developing cryptographic standards, and those empowered with the mandate to uncover threats to national security. In short, keep your lock-makers away from your lock-breakers.[48] To this point, Access organized a recent coalition letter signed by 30 companies and organizations and 5 noted technical experts, including Eleanor Saitta and Jacob Appelbaum.[49] The missive specifically explained that governments should empower a civilian agency to perform the "information assurance" functions, of helping to defend information systems, rather than leaving the lock-breakers in charge.[50]

Any country that works on information assurance should empower such an agency and keep it independent from any other agency that serves any surveillance function. The independent agency should receive its own adequate funding and resources. In addition, the agency should be empowered with sufficient technical expertise to allow it to operate on its own discretion rather than depending on other experts, like a life preserver, in order to serve its established function. Until governments institute changes like these, it is unlikely that users will be able to fully trust much of the internet's infrastructure, and or feel truly secure in the privacy of their personal transactions.

---

[48] See https://www.accessnow.org/blog/2014/09/18/virtual-integrity-the-importance-of-building-strong-cryptographic-standards for recommendations to US government authorities regarding cryptographic standards and safeguards.
[49] https://www.accessnow.org/page/-/Veto-CISA-Coalition-Ltr.pdf
[50] See https://www.accessnow.org/blog/2014/04/21/access-and-partners-call-on-nist-to-strengthen-cryptography-standards

Conclusion

The UK Parliament must carry out several essential reforms to regain its leadership on civil and political rights protections. Transparency from the government and by companies carrying out surveillance requests is key to communicating risks and rebuilding the trust of users in the businesses that hold their sensitive data. Data retention mandates violate fundamental human rights, and threaten the global competitiveness of UK firms, for no proven security benefit, and must be abolished. Finally, attention to cryptographic standards and the integrity of systems will ensure that all users remain secure and free to exercise their rights online.

In conclusion, Access reiterates our support for the Independent Reviewer's work and our intention to guide the Investigatory Powers Review toward effective and immediate outcomes for users at risk, worldwide.

***

Access (AccessNow.org) is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

For more information, please contact:
Peter Micek
Senior Policy Counsel
peter@accessnow.org
+1-888-414-0100 x709