Joint Representations by Access, the Center for Democracy & Technology, the Electronic Frontier Foundation, and New America's Open Technology Institute on "Interception of communications and equipment interference: draft codes of practice"

March 20, 2015
RIPA@homeoffice.x.gsi.gov.uk

I. Introduction

On February 6, 2015, the Home Office of the UK Government published two documents: an updated version of "Interception of Communications Code of Practice,"[1] and a new document, "Equipment Interference Code of Practice."[2]

The documents, together, provide guidance on the exercise of the authorities found in the Regulation of Investigatory Powers Act (RIPA) of 2000 (as modified by the Data Retention and Investigatory Powers (DRIP) Act of 2014),[3] the Security Services Act of 1989,[4] and the Intelligence Services Act of 1994.[5] These authorities are used by security and intelligence agencies, including the Government Communications Headquarters (GCHQ), the Security Service (MI5), and the Secret Intelligence Service (SIS), to conduct and facilitate surveillance.[6]

Though they purport to increase safeguards on intelligence agencies' exercise of their powers, these documents fail to assuage concerns about misuse and abuse by government officials. This is primarily because the documents fail to consider the ramifications of the technologies and capabilities sought and fail to properly respect the human rights of those impacted by their operation.

Specifically, the documents undermine the integrity of communications and systems utilized by people around the world, including those at risk of persecution and other serious abuses.[7] To the extent the draft Codes contain safeguards, they do not

---

[1] HOME OFFICE, INTERCEPTION OF COMMUNICATIONS CODE OF PRACTICE (2015) (draft for public consultation) [hereinafter ICCP].
[2] HOME OFFICE, EQUIPMENT INTERFERENCE CODE OF PRACTICE (2015) (draft for public consultation) [hereinafter EICP]. We note, this Code was mandated by RIPA in 2000, but only just published in 2015.
[3] Regulation of Investigatory Powers Act, 2000, c.23 (U.K.), *amended by* Data Retention and Investigatory Powers Act, 2014, c. 27 (U.K.) [hereinafter RIPA].
[4] Security Services Act, 1989, c. 5 (U.K.).
[5] Intelligence Services Act, 1994, c. 13 (U.K.) [hereinafter ISA].
[6] GOVERNMENT COMMUNICATIONS HEADQUARTERS, http://www.gchq.gov.uk/Pages/homepage.aspx (last visited March 19, 2015); THE SECURITY SERVICE, https://www.mi5.gov.uk/ (last visited March 19, 2015); SECRET INTELLIGENCE SERVICE, https://www.sis.gov.uk/ (last visited March 19, 2015).
[7] Modifying communications systems in order to facilitate surveillance undermines the secure use of those systems by all users. *See generally* Bruce Schneier, *Web Snooping is a Dangerous Move*, CNN

adequately limit the collection of data,[8] fail to take into account the need for adequate oversight mechanisms, give rise to a risk of serious breaches of lawyer-client privilege, neglect to consider the impact of these measures on the freedom of expression, and lack proper consideration of the impact on the human rights of those located outside the United Kingdom. Many of these potential human rights violations may be exacerbated by the secret data transfer arrangements between the UK and other countries, particularly the United States, Canada, Australia, and New Zealand (collectively, the "Five Eyes").

Equipment Interference Code of Practice

The Equipment Interference Code of Practice ("EI Code") applies to the authorization of equipment interference.[9] This expressly excludes any interference that involves the "consent of a person having the right to control the operation or the use of the equipment."[10] The separate security and intelligence agencies each use the authority slightly differently in line with their separate missions. While the framework expressly, albeit cursorily, takes into account Articles 6 and 8 of the European Convention on Human Rights ("Right to a fair trial" and "Right to respect for private and family life," respectively) and Article 1 of the First Protocol thereto ("Right to peaceful enjoyment of possessions") there is no discussion of the impact these activities could have on other human rights, such as the freedom of speech, the freedom of assembly, or the right to anonymity, as spelled out in the European Convention or other international instruments.[11]

The document further:

IREPORT, http://edition.cnn.com/2010/OPINION/09/29/schneier.web.surveillance/index.html (Sept. 29, 2010).

[8] Broadly speaking, in both documents intelligence collection is authorized so long as it is loosely related to national security, the prevention or detection of serious crime, or the economic well-being of the UK. The missions of the different agencies are further spelled out in Section 5 of the Intelligence Services Act of 1994, *available at* http://www.legislation.gov.uk/ukpga/1994/13/section/5.

[9] Defined as, "Any interference (whether remotely or otherwise) by the Intelligence Services, or persons acting on their behalf of (*sic)* in their support, with equipment producing electromagnetic, acoustic and other emissions, or information derived from or related to such equipment, which is to be authorized under section 5 of the 1994 Act, in order to do any or all of the following: (a) obtain information from the equipment in pursuit of intelligence requirements; (b) obtain information concerning the ownership, nature and use of the equipment with a view to meeting intelligence requirements; (c) locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b); (d) enable and facilitate surveillance activity by means of the equipment; "Information" may include communications content, and communications data as defined in section 21 of the 2000 Act." EI CODE, *supra* note 2, at ¶ 1.6.

[10] EICP, *supra* note 2, at fn. 5.

[11] European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, ETS 5 [also known as the European Convention on Human Rights; hereinafter ECHR].

- Sets forth the requirements for authorizing warrants, which need not necessarily specify the identity of the person targeted by the interference or the "details of any offense suspected or committed";[12]
- States that warrant applications should provide no additional information above what is expressly required by law;[13]
- Requires an assessment of any collateral intrusion and details of measures to limit it, but also expressly permits targeted interference against "individuals who are not intelligence targets in their own right" so long as the action is treated as intended intrusion;[14]
- Provides for the collection of legally privileged and other confidential information if so authorized;[15]
- Requires satisfactory arrangements in respect to the disclosure of information, yet does not detail how those arrangements will be enforced if disclosure is outside of the intelligence services;[16]
- Sets forth procedures for the review, amendment, and oversight of warrants, including:
    - Requires review of warrants on an on-going basis, at a frequency determined by the government official who applied for the warrant;[17]
    - A permissive requirement that a new application be filed for significant and substantive changes in the nature of the interference;[18] and
    - A permissive requirement for senior officials to be involved in overseeing the execution of a warrant;[19]
- Requires a database of warrants for a three-year period;[20] and
- Allows a single authorization for a "broad class of operations" when those operations are to be conducted on equipment located outside the UK or related to an apparatus that is or is believed to be outside the UK, or anything appearing to originate from that apparatus.[21]

Interception of Communications Code of Practice

The Interception of Communications Code of Practice ("IC Code") was originally published on September 8, 2002. As such, this document is an update from existing public policy, and here we only comment on additions to the document.[22]

---

[12] EICP, *supra* note 2, at ¶4.6.
[13] *Id.* at ¶ 2.16.
[14] *Id.* at ¶ 2.12.
[15] *Id.* at ¶ 3.1.
[16] *Id.* at ¶ 6.6. It is unclear if the disclosure anticipated here is intra-agency or international.
[17] *Id.* at ¶ 2.14.
[18] *Id.* at ¶ 2.15.
[19] *Id.* at ¶ 2.17.
[20] *Id.* at ¶ 5.1.
[21] *Id.* at ¶ 7.3.
[22] Omission of representations on content in the prior version does not indicate agreement on any provision or procedure.

This document "provides guidance on the procedures that must be followed before interception of communications can take place" under UK law.[23] Interception is unlawful under UK law, unless conducted under a warrant. The Interception code applies to the provider of any technology, including telecommunications services and internet services, and also includes updated provisions on provider assistance and provisions of interception capability.[24]

The document further:

- Removes many references to the need for reasonableness within the provider assistance provisions;[25]
- Expands the instances when a government official may unilaterally amend a warrant without approval;[26]
- Expands the section on guidance for (8)(4) warrants to expressly include bulk collection of any communications not contained wholly within the British Isles;[27]
- Provides new guidance regarding the service of warrants and notices on service providers outside the UK;[28]
- Adds express mention to the intelligence priorities set by the Joint Intelligence Committee ("JIC");[29]
- Places additional limitations on persons who can access intelligence information;[30]
- Requires biennial audits of activities by the Interception of Communications Commissioner.[31]

---

[23] Interception occurs when a party modifies or interferes with a system or its operation, monitors transmissions made by means of a system, or monitors transmissions made by wireless telegraphy to or from an apparatus comprised in a system in order to make some or all of the contents of the communication available while being transmitted to a person other than the sender or intended recipient. RIPA, *supra* note 3, at Ch. 1 Part 1.

[24] These updates are in response to changes made by the DRIP Act and expand the provisions expressly to companies that are outside the UK. The provisions are largely considered to be very harmful to individuals and to internet security. *See* Michael Rispoli, *No Slow DRIP: Expansion of Surveillance Powers Being Rammed Through Parliament,* PRIVACY INTERNATIONAL (July 15, 2014), https://www.privacyinternational.org/?q=node/299 ("This extra-territoriality power is a clear expansion of the existing regime, allowing the government to issue interception warrants to telecommunication companies and ISPs around the world. These companies would be compelled to not only assist in the interception of emails and phone calls, but also require backdoors to be built into communications infrastructure."). The provisions should not be reauthorized in 2016. *See* Shaheed Fatima, *U.K. Data Retention and Investigatory Powers Act 2014: Sticking Plaster or* Solution, JUST SECURITY (July 18, 2014 11:41 AM), http://justsecurity.org/13031/data-retention-investigatory-powers-act-2014-sticking-plaster-solution/.

[25] ICCP, *supra* note 1, at 3.11.

[26] *Id.* at ¶ 5.12.

[27] *Id.* at ¶ 6.4.

[28] *Id.* at ¶ 3.11.

[29] *Id.* at ¶ 6.8.

[30] *Id.* at ¶ 7.3.

[31] *Id.* at ¶ 10.2.

II. The tools and technologies implicated by equipment interference may have broad and unintended consequences

Historical legal frameworks for interception recognized it as one of the most intrusive possible investigative powers, due to the sensitive nature of real-time conversations. However, computer hacking and equipment interference can be even more intrusive and disruptive, encompassing ongoing control over a device or communications channel, covert changes to the platform performing communications, location tracking by using location sensors and systems that many modern devices have, contact tracking by collecting the social connections between a device and others it communicates with, recording audio and video of the device's surroundings, and facilitating impersonation using stored or forged credentials.

It has become increasingly clear that the computers and mobile devices have a critical role as repositories and tools for of all aspects of a person's life. Devices and equipment implicated by intrusion and interference include not merely personal computers and mobile devices but also computers in a connected home or office (surveillance cameras, security systems, connected appliances), computing devices embedded in vehicles such as automobiles, and communications servers and gateways that provide connectivity for large geographic areas and groups of people. Any technical interference with or intrusion onto these devices must be very carefully tailored to focus scrutiny and interference narrowly.

The power to interfere with and/or corrupt software to make it operate contrary to the intent of its users is much more insidious and far-reaching than the power to intercept private communications.[32] In the modern world, with extensive connectedness and embedded networked computation, the power to interfere with a device or the communications in which it participates is an open-ended and far-reaching authority that can easily frustrate standard operations, sabotage human intentions, and undermine human relationships. Further, corrupting or interfering with software can be a means of stealing money, destroying reputations, forging evidence, or injuring patients and passengers.

"Equipment interference" is not only about interception. Interception at its most basic level refers to passively capturing signals and data. Interference with equipment could go much farther to encompass modifying communications en route and even injecting malicious signals and software so that a previously secure communication channel can be bent to the will of those not engaged directly in the conversation.

It is inherently dangerous to engage in some of the types of interference with equipment that the EI Code would authorize. It appears to authorize *any* type of

[32] *See* the principle of "Integrity of Communications and Systems" in the widely endorsed INTERNATIONAL PRINCIPLES ON THE APPLICATION OF HUMAN RIGHTS TO COMMUNICATIONS SURVEILLANCE, *available at* https://en.necessaryandproportionate.org/ [hereinafter THE PRINCIPLES].

equipment interference that is engaged in for the purpose of obtaining information from the equipment, or obtaining information about the ownership, nature and use of the equipment. It includes modifying hardware or software to obtain such information.[33]

Interference permitted by the EI Code can take many forms and can be used by UK authorities to accomplish powerful control over persons or devices. Interference authorized under the EI Code in which UK authorities have already engaged includes, for example, defeating encryption protections[34] and executing denial of service attacks.[35] It could also include: (i) blocking or degrading access to information by means of one device or service, and (ii) causing a device or channel of communication to appear to be error-prone or und trustworthy, in order to encourage use of less secure devices and services more prone to eavesdropping. It could include theft of a person's communications device and substitution of another device the security of which has been compromised. All of these activities, even if engaged in for legitimate purposes, undermine trust in communications that is essential in our interconnected world. Worse still, they can be mimicked by malfeasors and used to commit financial fraud and theft.

The impact of "equipment interference" may not only be limited to individual devices. Devices are not isolated elements of our digital environment; they are networked and have many other dependencies. Many devices operate in roles of transitive trust, where a single device (like a smartphone) is used to establish authenticity to other devices, accounts, and communications channels (for example, many online financial institutions use a two-step login that requires the user to be able to receive a code via SMS (text) message on a trusted device to login to their account, in addition to a password).

Moreover, some systems are particularly sensitive, such that intrusion or interference may undermine the security of a whole class of devices, communication channels, or software programs; for example, systems that store cryptographic keying material – the keys and credentials that ensure the confidentiality and integrity of online secure transactions and communications – could allow surreptitious access to many disparate devices, identities, and services protected by those encryption keys, akin to gaining access to all the keys for every automobile in a parking structure. Intrusion and/or interference may also compromise

---

[33] EICP, *supra* note 2, at ¶1.6.
[34] James Ball, Julian Borger, and Glenn Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security," *The Guardian* (6 September 2013), *available at:* http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.
[35] Katie Collins, "Anonymous and LulzSec targeted by GCHQ DDoS attacks," *Wired UK* (5 February 2014), *available at:* http://www.wired.co.uk/news/archive/2014-02/05/gchq-ddos-attack-anonymous

communications infrastructure by destabilizing critical communication gateways – devices that route all communications in a geographic area or group of people.[36]

Interfering with a device or taking control of a computer effectively means reprogramming it to perform covert and harmful behaviors. The EI code permits interference with equipment that serves to "locate and examine, remove, modify or substitute equipment hardware or software,"[37] which effectively allows arbitrary control over devices subject to an interference warrant. This can encompass a wide variety of results from changing file contents (spreadsheets, word processing documents, other pieces of software), to ongoing surveillance (e.g., allowing a webcam to record when not activated by the user), sending data in the name of the user when they did not know or consent to that communication, attacking third parties by using the device as a platform to launch attacks, deleting data, and rendering the device inoperable.

Computers' general-purpose programmability means that computer intrusion is not intrinsically limited in scope, purpose, effect, or duration from a technical standpoint; computer intrusion tools may also permit software updates in order to apply new functionality/reprogramming long after the initial intrusion has occurred. Therefore, equipment interferences may not be "one-off" events, and instead may facilitate continuous or repeated human rights abuses of the kind described below. Thus, any limits on the invasiveness of these techniques must be limited externally through law and independent oversight.
The EI Code makes it clear that it is the responsibility of the Secretary to establish that activities are necessary for one or more statutory purposes, and proportionate to the aim of the warrant.[38] Such a consideration is also a requirement of international law when conducting communications surveillance.[39] However, the EI Code includes only procedures that include the consideration of a limited set of risks pertaining to privacy, such as the risk of intrusion into personal life,[40] or the risk of obtaining private information,[41] or the risk to confidential material.[42]

Given the above list of risks caused by equipment interference, any code that requires an examination of the necessary and proportional nature of the warrant must also consider the wider reach of the interference to intrude or manipulate the personal life of the target or others, and to the integrity of communication systems

---

[36] For example, it is reported that the US National Security Agency may have unintentionally taken the entire country of Syria off the global internet due to interfering with a device (Syria's internet gateway) for surveillance purposes. *See* Jacob Kastrenakes, *NSA Was Responsible for 2012 Syrian Internet Blackout, Snowden Says,* THE VERGE (Aug. 13, 2014), http://www.theverge.com/2014/8/13/5998237/nsa-responsible-for-2012-syrian-internet-outage-snowden-says.
[37] EICP, *supra* note 2, at ¶1.6(c).
[38] *See* EICP, *supra* note 2, at ¶¶ 2.4, 4.7.
[39] *See* THE PRINCIPLES, *supra* note 32.
[40] *See* EICP, *supra* note 2, at ¶ 2.9.
[41] *See id.*
[42] *See id,* at ¶ 3.1.

in general. Assessing some consequences will almost certainly require wider consultation than between the Home Office and those applying for the warrant, and potentially beyond that of the Intelligence Services Commissioner. Many of the side effects of equipment interference, particularly those of infrastructure operators, have consequences that will be apparent only to experts knowledgeable in maintaining such infrastructure.

While the details of a particular warrant may require confidentiality in order to protect ongoing operations, "equipment interference" permits such a wide range of techniques that it should be possible to generically define individual strategies and consult with external sources to gauge potential risks of these actions. Only with such consultation will the EI Code be able to comply with its own requirements, and that of international law.

Many acts of interference exploit lapses or errors in existing digital security systems protecting individuals. For instance, in order to remotely seize control of a personal computer, intelligence and security services take advantage of a previously unknown error in the programming of those personal computers' security systems.

Such vulnerabilities are also exploited by criminals and agents of foreign powers and some flaws are so severe as to create serious risk of disabling or subverting critical infrastructure.[43] The U.S. claims to have internal procedures for determining whether such flaws should be disclosed to parties capable of mitigating or correcting the issue.[44] Such procedures should be part of the public code of practice, as unless they are publicly detailed in the EI code, it is impossible for the Minister to comply with the requirement that the act of interference be necessary and proportionate.

Questions for Consideration:

1. Does the Home Office appropriately distinguish between passive interception of information and active interference with devices?
2. While the IC/EC codes recognize the potential for collateral intrusion – where signals from innocent parties may be unintentionally or intentionally captured as a means to a lawful end – why does the code not also recognize the potential for collateral instability or damage with interference of devices?
3. What protections are in place to ensure that once a device is interfered with for surveillance purposes, the method of interference isn't subsequently used maliciously to impersonate the user, attack other devices, commit fraud, or damage other networked devices?
4. Does the Home Office contemplate performing non-surveillance tasks with intrusion or interference? Does the intrusion-as-information-capture

[43] *See* THE HEARTBLEED BUG, http://heartbleed.com/ (last visited March 19, 2015).
[44] *See* David E. Sanger, *Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say*, NEW YORK TIMES, and (April 12, 2014), *available at* http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html?_r=0.

perspective of the current IC/EC codes adequately provide safeguards in the public interest in those cases?

5. Does the Home Office take the position that intrusion or interference for non-surveillance purposes should be prohibited, except in cases of emergency when there is imminent risk of danger to human life?
6. Whose external technical advice will the Home Secretary use to determine the magnitude and scope of interference techniques, and therefore the degree of proportionality to what is sought to be achieved?
7. How does the Code of Practice intend to balance the advantages of pursuing an individual act of interference via a discovered security flaw, as opposed to protecting national security and the prevention acts of serious crime achieved by taking steps to mitigate or fix the flaw?
8. What methods will the Home Secretary use to review the impact of acts of equipment interference, and incorporate these wider consequences into considerations of the legality of ongoing and future warrants?

III. The impact on human rights, including rights of those outside the UK, is unacceptable

a. Extraterritorial interceptions and equipment interferences may violate international law

Under customary international law, which is binding upon the United Kingdom,[45] the State is prohibited from "*exercis[ing] its power in any form in the territory of another State.*"[46] This prohibition extends to any direct or indirect intervention in "*internal or external affairs of other States*."[47]

It is therefore our view that any UK warrants or authorizations that purport to allow UK intelligence or law-enforcement agents to exercise interception, equipment-interference or other powers in the territory of any other State (or in a manner that otherwise interferes either directly or indirectly in the affairs of that State) violate international law.[48] As an alternative, where the Secretary of State believes that interception or equipment interference in the territory of another State is both strictly necessary and proportionate, we submit that the Secretary should pursue formal criminal cooperation and diplomatic channels to obtain the consent of the relevant State. As explained below, however, we believe that authorities must nevertheless comply with the requirements of human rights law.

---

[45] *See* R v. Jones, [2007] 1 AC 136, ¶ 11.
[46] The Case of the S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, 18 (Sept. 27).
[47] Military and Paramilitary Activities in and against Nicaragua (Nicar. v U.S.), 1986 I.C.J. 14, ¶ 205 (June 27).
[48] *See* letter from the Center for Democracy & Technology to David Anderson, Independent Reviewer of Terrorism Legislation (10 October 2014), *available at* https://cdt.org/insight/submission-of-evidence-to-uk-investigatory-powers-review/.

b. Extraterritorial interceptions and equipment interferences may also violate the UK's human rights obligations

We note with grave concern that the RIPA as well as the EI Code and the IC Code provide (or could be read to provide) different levels of fundamental rights protections depending on the location of the sender and recipient of a communication or the location of the relevant equipment.

For example, the fact that RIPA imposes a far more relaxed standard for obtaining Section 8(4) warrants for the interception of "external" communications, compared with the requirements for obtaining Section 8(1) warrants for the interception of "internal" communications, are well known.[49] Moreover, as the draft IC Code now explicitly concedes, a warrant for the interception of "external" communications issued pursuant to Section 8(4) of RIPA could authorize the bulk collection of "all communications transmitted on a particular route or cable" or carried by a particular communications service provider ("CSP"); in other words, potentially billions of communications daily, including both content and communications data.[50] Such "external" communications may include those either sent *or* received by people within the UK, as well as those that take place solely between correspondents outside of the country.[51]

By contrast, the interception of communications between a sender and recipient who are both in the UK at least theoretically requires a warrant under Section 8(1) of the RIPA that specifies a single person or set of premises as the target of the interception activities. (Notably, however, the IC Code concedes that even these "internal" communications may potentially be collected through the dragnet surveillance regime meant to apply to "external" communications).[52] In addition, in response to legal challenges, the government has stated that it treats searches on Google and YouTube, posts on Facebook, and tweets as "external communications," since the companies' web servers are largely based outside the British Islands. This classification only increases the risk of disproportionate collection.

The UK is unquestionably obligated under the European Convention on Human Rights ("ECHR") and the Human Rights Act of 1998 to respect the human rights—

---

[49] *E.g., compare* Liberty and Others v the United Kingdom, [2008] All ER (D) 09 (Jul), ¶ 64, *with* Kennedy v the United Kingdom, 2010 Eur. Ct. H.R. 682.

[50] ICCP, *supra* note 1, at ¶ 6.2; *cf.* Ewen MacAskill et al., *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, THE GUARDIAN (June 21, 2013), *available at* http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (describing the volume of data GCHQ is able to collect by tapping fibre-optic cables); CENTER FOR DEMOCRACY & TECHNOLOGY AND AMERICAN CIVIL LIBERTIES UNION, "SECRET SURVEILLANCE: FIVE LARGE-SCALE GLOBAL PROGRAMS" (2014), ¶¶ 36-38, *available at* https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/09/cdt-aclu-upr-9152014.pdf (discussing the volume of communications that may be captured through the tapping of cables that connect CSP data centers).

[51] ICCP, *supra* n. 1, at ¶¶ 6.3-6.4.

[52] RIPA, *supra* note 3, at § 8(1); ICCP, *supra* note 1, at ¶¶ 6.6-6.7.

including the privacy, free expression, fair trial and other rights—of everyone within the State's jurisdiction.[53] This jurisdiction plainly includes any person within UK territory, regardless of where the other party to any relevant correspondence may be located.

Moreover, as the UN Office of the High Commissioner for Human Rights ("OHCHR") has found, "digital surveillance … may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure."[54] The OHCHR has also strongly implied that providing weaker human rights protections for foreigners or persons outside of a State's territory than for citizens or those within the territory will violate both the substantive and non-discrimination provisions of the relevant human-rights treaties.[55] The European Court of Human Rights has not reached any contrary findings in respect of surveillance activities, including in its decision in *Weber and Saravia v. Germany*, which did not reach the issue.[56] Particularly in light of the OHCHR's conclusions, the UK is in breach of its human rights obligations whenever it violates the privacy or other rights of people outside of the UK or provides weaker protections for them under its secret surveillance laws.[57]

c. The authorisation, renewal and oversight procedures found in RIPA and the Codes do not comply with human rights

The RIPA, the ISA, and the EI and IC Codes confer upon the Secretary of State the power to issue or renew the warrants or authorisations described in the legislation.[58] Prior to doing so, she is obligated to consider, *inter alia*, the necessity and proportionality of the secret surveillance measures involved (although, as noted above, the Home Office does not appear to believe that the Secretary of State is required to consider proportionality as such when issuing authorizations under Section 7 of the ISA).[59]

Whilst we support the prominence with which necessity and proportionality considerations are discussed in both the EI and IC Codes, the risk of unnecessary or disproportionate surveillance pursuant to RIPA, ISA, and the Codes is so manifest, particularly in respect to bulk collection or large-scale, invasive equipment interference activities, that the authorisation, renewal, amendment, and oversight of

---

[53] ECHR, *supra* note 11, at Art. 1; Human Rights Act 1998, c. 42 (U.K.).
[54] Office of the United Nations High Commissioner on Human Rights, *The Right to Privacy in the Digital Age*, ¶ 34 UN Doc. A/HRC/27/37 (June 30, 2014) (hereinafter "OHCHR report").
[55] *Id.* at ¶¶ 35-36.
[56] *See* Weber and Saravia v Germany, 2006-XI Eur. Ct. H.R., ¶¶ 87-88.
[57] For further discussion, *see* SCOPE: EXTRA-TERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES, https://en.necessaryandproportionate.org/LegalAnalysis (last visited March 19, 2015).
[58] RIPA, *supra* note 3, at §§ 7, 9; ISA, *supra* note 5, at §§ 5-7; EICP, *supra* note 2, at ¶¶ 2.2, 4.11, 7.5; ICCP, *supra* note 1, at ¶ 3.4.
[59] EICP, *supra* n. 2, at ¶¶ 2.4-2.12; ICCP, *supra* note 1, at ¶¶ 3.5-3.6.

the relevant warrants and authorizations should be entrusted to an entity independent of the bodies conducting the surveillance in order to ensure compliance with the ECHR.[60]

Although the implementation of UK surveillance laws are subject to independent oversight at the highest level, it is inconsistent with the Convention and the rule of law more broadly for the Secretary of State to enjoy such vast and plenary powers to order and, in the most routine and immediate sense, oversee the implementation of surveillance measures that may affect hundreds of millions of individuals both within and outside the UK. To provide meaningful safeguards against abuse, we urge the Home Office and the Parliament to create a system of authorization and oversight that is sufficiently independent of the surveilling bodies to uphold the Convention rights of each individual affected, as well as sufficiently expert in the relevant technologies to understand the full implications of the measures authorized. We note the European Court's prior indication that "in a field [i.e. secret surveillance] where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge."[61]

d. RIPA and the Codes facilitate unnecessary and disproportionate surveillance of third parties

Articles 8 and 10 of the ECHR, which concern the rights to privacy and freedom of expression respectively, require that any interference with these rights must be "necessary in a democratic society" for certain specified purposes. The European Court of Human Rights has repeatedly emphasized that this necessity requirement, which is sometimes described in terms of proportionality, means that secret surveillance is "tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions."[62] The Court has also explicitly stated that the term "necessary" must be narrowly construed, and the word cannot be interpreted to mean merely "reasonable."[63] Meanwhile, the OHCHR has suggested that "mass" or "bulk" surveillance activities, in particular, give rise to a serious risk of violations of these standards.[64]

See, e.g., Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, 2007-III Eur. Ct. H.R., ¶¶ 85-89; Popescu v. Romania (No 2), 2007-III Eur. Ct. H.R., ¶¶ 70-73. Where equipment interferences are concerned, we note that the EICP explicitly acknowledges that a single authorisation "may relate to a broad class of operations." EICP, *supra* note 2, at ¶ 7.11.

[61] Klass and Others v. Germany, 2 Eur. H.R. Rep. 214, ¶ 56 (1978).
[62] *Id.* at ¶ 42; Rotaru v Romania, 2000 Eur. Ct. H.R. 192, ¶ 47; Dragojević v Croatia, 2015 Eu. Ct. H.R., ¶ 97.
[63] Klass, 2 Eur. H.R. Rep. 214, at ¶ 42; Handyside v the United Kingdom, 1976 Eur. Ct. H.R. 5, ¶ 48.
[64] OHCHR report, *supra* note 51, at ¶ 25; For further discussion of the application of international law to mass surveillance, see PRINCIPLES 3, 4 AND 5: NECESSITY, ADEQUACY AND PROPORTIONALITY, https://en.necessaryandproportionate.org/LegalAnalysis/principles-3-4-and-5-necessity-adequacy-proportionality (last visited March 19, 2015).

We support the assertion found in the EI Code that, "[t]he fact that there is a potential threat to national security (for example) may not alone render the most intrusive actions proportionate" and that interferences will not be proportionate if "the information which is sought could reasonably be obtained by other less intrusive means."[65] However, several of the surveillance practices permitted under RIPA, the ISA, and the Codes of Practice entail an exceptionally grave risk of interferences with privacy and free-expression rights that do not meet the strict necessity standard found in the Convention (as interpreted by the Court).

In particular, it is difficult to reconcile the IC Code's rather blithe reference to the possibility that a Section 8(4) warrant could authorize "the interception of all communications transmitted on a particular route or cable, or carried by a particular CSP" with the Court's demand that all secret surveillance be "*strictly necessary for safeguarding the democratic institutions*" (see above). In this respect, we recall the Court's finding in *Liberty and others* that a UK legal regime under which "in principle, any person who sent or received any form of telecommunication outside of the British Islands … could have had such a communication intercepted" violated Article 8 of the Convention.[66]

We are also concerned about the references found in the Codes of Practice to "collateral intrusions" and "equipment interference activity specifically against individuals who are not intelligence targets in their own right."[67] The Home Secretary has not offered a sufficient explanation as to the types of circumstances in which such activities might be necessary and proportionate, especially in light of the highly restrictive manner in which the Court has construed the term "necessary." This failure to explain the types of circumstances that might lead a suspicionless party to be surveilled also contravenes the Court's requirement that the law be "*sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to [secret surveillance] measures*."[68]

e. The Codes of Practice fail to consider the freedom of expression

Although the Codes of Practice discuss the surveillance of journalists and their sources at some length, they do not explicitly mention the freedom of expression found in Article 10 of the ECHR and do not consider the impact of the permitted surveillance measures on the free-expression rights of individuals who are not connected with journalism. In light of the fact that secret surveillance may be unlawful if it unnecessarily or disproportionately burdens the freedom of

[65] EICP, *supra* note 2, at ¶ 2.6.
[66] Liberty and Others v the United Kingdom, [2008] All ER (D) 09 (Jul), ¶ 64.
[67] EICP, *supra* note 2, at ¶¶ 2.9-2.12; ICCP, *supra* note 1, at ¶ 4.1.
[68] Weber and Saravia v Germany, 2006-XI Eur. Ct. H.R., ¶¶ 87-88.

expression, we urge that the Codes be re-drafted, and the practices of the Home Office and the intelligence agencies updated, to take full account of this right.[69]

Even where journalists and their sources are concerned, the Codes come up short. Both the EI and IC Codes effectively concede that the authorities might intentionally target "confidential information," including that shared between sources and journalists.[70] The European Court of Human Rights has stated that journalists and sources enjoy a heightened level of protection under Article 10 of the Convention, and that limitations on these individuals' free-expression rights will be subject to "*the most careful scrutiny*" by the Court.[71] The same legality and foreseeability requirements apply as under Article 8, and although the Court was willing to accept that a mass surveillance programme that did not intentionally target journalists or sources complied with the Convention, it reached the opposite result in a case that involved "the targeted surveillance of journalists in order to determine from whence they ha[d] obtained their information."[72] Thus, we believe that the Codes' indication that the UK authorities may intentionally target journalists (combined with a general lack of foreseeability of the kinds of circumstances in which this might occur) means that the Home Office proceeds at its peril in this respect.[73]

f. The Codes of Practice mischaracterize and facilitate violations of the lawyer-client privilege

The Codes of Practice fundamentally mischaracterize the range of communications that may be subject to legal privilege in the UK as well as the nature of the privilege itself. As a result, they facilitate violations of Article 8 of the ECHR.

The European Court of Human Rights has long since established that lawyer-client communications are "specifically protected" by Article 8, and that by virtue of that provision, "correspondence between a lawyer and his client, whatever its purpose … enjoys privileged status where confidentiality is concerned."[74] Although this protection is not absolute, the Court "attaches particular weight" to it, since interferences "may have repercussions on the proper administration of justice."[75] As the Court has observed: "[L]awyers are assigned a fundamental role in a democratic society, that of defending litigants. Yet lawyers cannot carry out this essential task if they are unable to guarantee to those they are defending that their

[69] ECHR, *supra* note 11, at Art. 10.
[70] EICP, *supra* note 2, at ¶¶ 3.23-3.24; ICCP, *supra* note 1, at ¶¶ 4.2-4.3.
[71] Nordisk Film & TV A/S v. Denmark, 2005-XIII Eur. Ct. H.R.; Financial Times Ltd and others v the United Kingdom, 2009 Eur. Ct. H.R. 2065, ¶¶ 59-60.
[72] *See* Sunday Times v the United Kingdom (No 1), 2 Eur. H.R. Rep. 245, ¶¶ 46-49 (1979-80 Weber and Saravia v Germany, 2006-XI Eur. Ct. H.R., ¶¶ 145-153; Telegraaf Media Nederland Landelijke Media BV and others v the Netherlands, 2012 Eur. Ct. H.R., ¶ 97.
[73] Telegraaf Media, 2012 Eur. Ct. H.R., at ¶ 98.
[74] Michaud v France, 2012 Eur. Ct. H.R., ¶¶ 117, 119.
[75] *Id*.

exchanges will remain confidential. It is the relationship of trust between them, essential to the accomplishment of that mission, which is at stake."[76]

However, the EI and IC Codes permit the Secretary of State to issue a warrant for interception or equipment interferences that are "likely or intended to result in the acquisition of knowledge of matters subject to legal privilege."[77] Although the Codes impose certain limitations upon the types of circumstances in which the Secretary of State may order such actions, broad grounds (such as "in the interests of national security or the economic well-being of the UK") remain available.[78] Moreover, the Codes contemplate the "[t]he retention of legally privileged material, or its dissemination to an outside body."[79]

The relevant provisions state that such retention or sharing "should be accompanied by a clear warning that [the material] is subject to legal privilege" and that privileged material "should be safeguarded by taking reasonable steps to remove the risk of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates."[80] In our view, such warnings and ostensible safeguards are entirely beside the point. Legally-privileged materials cannot be intercepted, viewed, used, or retained by, or shared with, any entity other than the lawyer or client, save in the extremely narrow circumstances for disclosures that are recognized in democratic societies and permitted under the European Court of Human Rights' heightened standard.[81] To purport to provide otherwise is to defeat both the substance and purpose of the privilege, which the Court has explicitly identified as an essential component of the right to privacy.

Questions for Consideration:

1. How will the Secretary of State ensure that any surveillance activities conducted outside the territory of the UK or the Crown dependencies respect the binding customary international laws demanding strict respect for state sovereignty?
2. Does the Secretary of State believe that the provision of fewer human rights protections to people in the UK who happen to be parties to external communications than to those who do not take part in such communications is consistent with the UK's obligations under the human rights instruments? How will the Home Office ensure that it strictly complies with its Convention

---

[76] *Id.* at ¶ 118.
[77] EICP, *supra* note 2, at ¶ 3.7; ICCP, *supra* note 1, at ¶¶ 4.2-4.11.
[78] EICP, *supra* note 1, at ¶ 3.7.
[79] *Id.* at ¶ 3.16; ICCP, *supra* note 1, at ¶¶ 4.12-4.13. We support the ICCP's apparent imposition of a requirement to seek legal guidance (¶ 4.13) when handling or retaining intercepted materials that may be subject to legal privilege; however, we believe this requirement does not cure the other potential human rights violations described in this section of our submission.
[80] EICP, *supra* note 2, at ¶¶ 3.16-3.17; ICCP, *supra* note 1, at ¶¶ 4.14-4.15
[81] *See, e.g.*, Michaud, 2012 Eur. Ct. H.R.; Roemen and Schmit v Luxembourg, 2003 Eur. Ct. H.R., ¶¶ 70-72.

obligations in respect of such persons? Does the Home Office recognize that it owes human rights obligations to people outside of the UK where surveillance activities are concerned?

3. What is the Home Secretary's justification for declining to propose a system of judicial authorisation and overall control (aside from the Investigatory Powers Tribunal) of secret surveillance activities?
4. How does the Home Office reconcile the possibility of "the interception of all communications transmitted on a particular route or cable, or carried by a particular CSP" with the requirements of necessity and proportionality set out in Articles 8 and 10 of the ECHR?
5. Will the Home Office provide an analysis of the consistency of the surveillance measures described in RIPA, the ISA and the relevant Codes of Practice with Article 10 of the ECHR?
6. In the Home Office's view, what is the scope of the legal privilege under both the ECHR and domestic law, and on what grounds does the Home Office believe that the provisions of the Codes of Practice addressing the interception, handling, retention or dissemination of privileged materials (particularly, but not exclusively, as a result of bulk collection practices) comply with these laws?

IV. There is inadequate information available concerning the dissemination of information to states and governments outside the UK

Wide-ranging information sharing agreements exist between various countries' intelligence agencies, such as the agreement between the "Five Eyes."[82] However, little is known about how information is collected and with whom that information is shared. Documents suggest that in addition to the formal information sharing agreement with the Five Eyes, the UK Government may also be a party to other formal and informal information sharing agreements. Intelligence agencies share both select interceptions and raw data with non-Five Eyes countries such as Israel.[83]

Despite the vast scope of its information collection and sharing practices, the UK Government has not disclosed adequate information concerning what safeguards it has in place to ensure that neither it nor the foreign intelligence agencies with

---

[82] *See, e.g.,* Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASHINGTON POST, Oct. 30, 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html; Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, & James Ball, *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, THE GUARDIAN, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[83] Glenn Greenwald, *Cash, Weapons and Surveillance: the U.S. is a Key Party to Every Israeli Attack*, THE INTERCEPT, Aug. 4, 2014, https://firstlook.org/theintercept/2014/08/04/cash-weapons-surveillance/.

whom it shares information use that information to commit human rights abuses. Further, it is not clear that there is any limitation on sharing of information that lacks a nexus to national security threats. These information-sharing practices may violate both domestic and international laws.

The information sharing agreements raise further questions because they may facilitate the receipt of surveillance information that a government may not be able to obtain under its own laws. This is because the UK authority is more expansive than that of many other countries, including the United States in many instances. For example, authorities in the DRIP Act intended to facilitate information collection go beyond the authorities granted under U.S. law.

Two provisions in the IC were updated to reflect changes made by the DRIP Act in 2014. Both the section of "provision of reasonable assistance" and the "provision of intercept capability" now expressly apply to companies that do business outside the UK, so long as they have UK customers. While both sections are problematic, the provision of interception capability is particularly troubling. The section obligates telecommunications companies to, if requested, "provide a permanent intercept capability." In UK law, telecommunications companies include internet content providers as well.

The equivalent U.S. statute is the Communications Assistance for Law Enforcement Act (CALEA), which requires that telephone companies, internet broadband providers (like internet service providers), and some voice over internet protocol (VoIP) providers design their network architectures in a manner that enables law enforcement to easily wiretap communications that transit those services.[84]

While there have been attempts to expand CALEA to require all communications services to weaken the security of their products in order to enable U.S. government surveillance,[85] those proposals have been rejected by lawmakers. They have come under sharp criticism by security experts because it is impossible to weaken a product's security protocols to enable government access without undermining the security of the product such that the vulnerabilities intended only for legitimate government uses could be exploited by malicious actors as well.[86]

---

[84] Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1002 (1994); *see also* FED. COMMC'N COMM'M, ET DOCKET NO. 04-295, FIRST REPORT AND ORDER AND FURTHER NOTICE OF PROPOSED RULE MAKING (2005), *available at* https://net.educause.edu/ir/library/pdf/EPO0528.pdf.

[85] Charlie Savage, *U.S. Is Working To Ease Wiretaps On the Internet*, NY TIMES, Sept. 27, 2010, http://query.nytimes.com/gst/fullpage.html?res=9E03E4D61030F934A1575AC0A9669D8B63&ref=charlie_savage&pagewanted=1&pagewanted=all; *and* David E. Sanger & Matt Apuzzo, *James Comey, F.B.I. Director, Hints at Action as Cellphone Data Is Locked*, NY TIMES, Oct. 16, 2014, http://www.nytimes.com/2014/10/17/us/politics/fbi-director-in-policy-speech-calls-dark-devices-hindrance-to-crime-solving.html.

[86] *See* Adida et al., CALEA II: RISKS OF WIRETAP MODIFICATIONS TO ENDPOINTS (2013) (a technical report from 20 leading security and cryptography experts), *available at* https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf; THE #CRYPTODEBATE BIBLIOGRAPHY, NEW AMERICA'S OPEN TECH. INST. (2014), *available at*

Questions for Consideration:

1. What information sharing agreements exist between the UK and other countries, allowing either raw or processed information collected by means of government surveillance to be transferred to other countries? What safeguards do these agreements require?
2. Are there any restrictions in place to prevent the transfer of information to a State that would be otherwise prohibited from collecting the information in the first instance under its own laws and regulations?
3. Has there been a study on the feasibility of requiring cross-border data requests for intelligence information to be sought through the Mutual Legal Assistance Treaty process, which builds in safeguards for human rights and protections from abuse?

V. Conclusion

Thank you for the opportunity to comment on these documents. As you consider these documents, we believe it is important for all stakeholders to articulate specific and meaningful objections. If you have any comments or questions, please direct them to Amie Stepanovich, U.S. Policy Manager at Access [amie@accessnow.org] and she will communicate them to the rest of the coalition.

---

http://www.newamerica.org/downloads/OTI_CryptoDebate_Bibliography.pdf; *see also Debate on Law Enforcement vs. Smartphone Encryption: Is FBI "Going Dark" or in a Golden Age of Surveillance?*, NEW AMERICA'S OPEN TECH. INST., Nov. 17, 2014, http://www.newamerica.org/oti/debate-on-law-enforcement-vs-smartphone-encryption/; *and see* Danielle Kehl, Kevin Bankston, & Andi Wilson, COMMENTS TO THE UN SPECIAL RAPPORTEUR ON FREEDOM OF EXPRESSION AND OPINION REGARDING THE RELATIONSHIP BETWEEN FREE EXPRESSION AND THE USE OF ENCRYPTION, NEW AMERICA'S OPEN TECH. INST. (2015), *available at* https://static.newamerica.org/attachments/1866-oti-urges-un-human-rights-council-to-promote-the-benefits-of-strong-encryption/OTI_Crypto_Comments_UN.pdf.