Privacy and Security Inquiry
Intelligence and Security Committee of Parliament
35 Great Smith Street
London, SW1P 3BQ

Executive Summary

This comment is submitted on behalf of Access (www.accessnow.org), an international organization that defends and extends the digital rights of users at risk around the world. We appreciate this opportunity to input into the Intelligence and Security Committee of Parliament (ISC) inquiry[1] into surveillance laws and practices.

In this comment, Access will express 1) the need for an unrestricted and open inquiry into this complex and challenging issue; 2) the growing international agreement that distinguishing between content data and metadata is no longer appropriate; and 3) that, without more information on current surveillance practices, the public cannot yet debate the specific legal and policy steps that the government should take to better meet its human rights obligations.

Based on the limited information released to date on surveillance practices of the United Kingdom, we see the need for a robust public debate on the scale and scope of surveillance taking place. Reports suggest that fundamental human rights are impacted daily, in the UK and abroad, by the government, its intelligence agencies, and the companies that take part, willingly or otherwise, in its operations. Any Parliamentary or other government inquiry should welcome a broad set of perspectives and evidence on this wide-ranging, far-reaching surveillance capability that threatens so many fundamental rights and liberties.

Unfortunately, we have concerns about the legitimacy of this inquiry as it is currently framed. We find the questions biased and unnecessarily restricted in their scope. Suggesting that society must choose between individual privacy and "collective" security, for example, puts the two values in opposition to one another, despite evidence that privacy and security are mutually reinforcing in the digital environment. For example, websites that encrypt communications with their users by default maintain the confidentiality of those communications, while also protecting both the user and corporate servers from intrusions. Moreover, the framing of a "collective right" to security does not appear to be grounded in law, distracting from the sober legal conversation that must take place on communications surveillance.

[1] https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20131211_ISC_Call_for_papers-Privacy.pdf

This inquiry is not the first to take place following revelations of mass surveillance, and should seek to build on those reviews that other governments have completed. We offer key insights from those reviews, including that communications metadata should be protected as least as strongly as content data is, and that bulk collection violates human rights and offends the principles of democratic society. As a solution, we refer the Committee a set of international principles applying human rights frameworks to government surveillance.

Finally, we submit that more transparency is needed from the government as well as from corporations on the extent of surveillance taking place. Disclosure of this information is a prerequisite to the public debate that crucially must take place on reforming the UK surveillance regime, and which is necessary to more adequately protect the rights of users in the UK and elsewhere.

What balance should be struck between the individual right to privacy and the collective right to security?

1. This question assumes that protections for an individual's privacy somehow threaten security. We reject this framing as biased. Assuming the need to "balance" these rights suggests presents a Faustian trade-off between security and privacy, suggesting that one must be sacrificed in order to have more of the other. This is a false juxtaposition.

2. **Rather, privacy and security are mutually reinforcing values.**

3. Evidence has shown that the values of security and individual privacy are mutually reinforcing in the online environment. As reports from the Guardian show, intelligence agencies including the NSA and GCHQ increasingly introduce new vulnerabilities into the internet's architecture.[2] For example, encryption standards purposefully weakened by intelligence agencies can be exploited by all parties who discover these security vulnerabilities, or "back doors," not solely by government agents. These vulnerabilities not only threaten individual privacy, but also weaken the integrity and security of this globally shared resource.

4. Other voices have weighed in with persuasive arguments against such "balancing." The United States President's Review Group on Intelligence and Communications Technologies found the idea of balancing security and rights can be "inadequate and

[2] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

misleading."[3]

5. The President's Review Group wrote,

> some safeguards are not subject to balancing at all. In a free society, public officials should never engage in surveillance in order to punish their political enemies; to restrict freedom of speech or religion; to suppress legitimate criticism and dissent; to help their preferred companies or industries; to provide domestic companies with an unfair competitive advantage; or to benefit or burden members of groups defined in terms of religion, ethnicity, race, and gender.[4]

6. This statement outlines the adverse impacts that surveillance can have on a range of human rights, and the danger of "mission creep," or the risk that the purposes of surveillance can shift quickly and easily toward unlawful ends. Revelations exposed by the Guardian and other news sources have illustrated that once such surveillance capabilities are established, they become difficult to control.[5]

7. **There is no legal grounding for a 'collective right' to security.**

8. The consultation's first question refers to "the collective right to security." Leaving aside concerns on who can assert a collective right, what is the scope of the right, and how is it violated, Access asserts that no "collective right to security" exists in the legal sense.

9. For example, privacy is recognized in Art. 7 of the EU Charter of Fundamental Rights,[6] which reads, "Everyone has the right to respect for his or her private and family life, home and communications." Security is affirmed in Art. 6: "Everyone has the right to liberty and security of person." Thus, the right to security is prefaced by the same phrase as the *individual* right to privacy: "Everyone has the right to…" and ends with the phrase "security of person," which may be interpreted as referring to an individual.

10. It is not clear why the Committee refers to the right to security using the vague terminology "collective right." This extra-legal language serves to de-legitimize this consultation process and distract from a legally grounded discussion of the

---

[3] http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (at 16)
[4] http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (at 16)
[5] http://www.theguardian.com/world/2013/nov/18/surveillance-technology-out-of-control-ashdown
[6] http://www.eucharter.org/home.php?page_id=14

fundamental right to privacy in the digital era.

11. With this question, the Committee likely seeks to address the proportionality of harms resulting from communications surveillance. For a better framing, we suggest the Committee study the International Principles on the Application of Human Rights to Communication Surveillance[7] (also known as the Necessary and Proportionate Principles).

12. The Necessary and Proportionate Principles resulted from a global consultation with civil society groups, industry, and international experts in communications surveillance law, policy, and technology. More than 330 civil society groups have signed onto the Principles, which provide a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights.

13. Under the principle of Proportionality, decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's human rights, and to other competing interests. These decisions should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy, and be made in accord with the procedural safeguards elaborated in the Necessary and Proportionate Principles.[8]

14. **The scope is too limited.**

15. As a plethora of other parliamentary and executive reviews have undertaken over the past six months, the issue of surveillance of digital communications in national, regional, and international anti-terrorism efforts is complex, challenging, and deserving of more than passing inquiries. Access believes this consultation barely scratches the surface of what is clearly a systemic and immensely complicated subject, and that a robust debate would require much more data and open briefings by the UK government and its intelligences services.

16. Examples of better lines of inquiry can be found in other recent reviews that governments and institutions have undertaken. In a series of 15 hearings, for example, the European Parliament's Committee on Civil Liberties (LIBE) undertook to investigate the effects of surveillance on fundamental rights, in particular the rights of data protection and respect for private life, freedom of expression, the

[7] http://necessaryandproportionate.net
[8] https://en.necessaryandproportionate.org/text

presumption of innocence, and effective remedy.[9] The Committee recently presented its draft report[10] on the impact of mass surveillance programmes on the rights of European citizens, condemning mass surveillance programs "in the strongest possible terms."[11]

17. Concurrently, two review bodies in the United States, the Privacy and Civil Liberties Oversight Board (PCLOB)[12] and the President's Review Group on Intelligence and Communications Technologies,[13] issued comprehensive reports calling for an end to mass collection of the communications metadata of US persons, among other recommendations.

18. This Committee's inquiry could build on those deep and broad reviews by shedding light on the opaque body of UK government surveillance policies and practices, and provide context to the reports appearing in news media. However, in its current form the consultation is too limited to achieve this goal.

To what extent might it be necessary and proportionate to monitor or collect innocent communications in order to find those which might threaten our security? How does the intrusion differ between data (the fact a call took place between two numbers) as opposed to content (what was said in the call)?

19. **The traditional distinction between content data and metadata is no longer appropriate.**

20. These categories of data types are no longer appropriate for measuring the degree of the intrusion that communications surveillance makes into individuals' private lives and associations. With the depth of surveillance taking place, the acquisition of metadata can reveal the personal relationships, political leanings, or daily routine of a person. The extent of metadata acquisition, therefore, can be as revealing as the content itself. This reasoning is reflected in the findings of the US PCLOB report, which found, "The circumstances of a particular call can be highly suggestive of its content, such that the mere record of a call potentially offers a window into the

[9] http://www.europarl.europa.eu/news/en/news-room/content/20130708IPR16833/html/Civil-Liberties-Committee-MEPs-agree-on-surveillance-inquiry%27s-next-steps
[10] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-526.085%2b02%2bDOC%2bPDF%2bV0%2f%2fEN
[11] https://www.accessnow.org/blog/2014/01/22/ep-inquiry-presents-its-plan-for-the-future-to-protect-citizens-against-mas
[12] http://www.pclob.gov
[13] http://www.dni.gov/index.php/intelligence-community/review-group

caller's private affairs"[14].

21. Likewise, the President's Review Group cited the Necessary and Proportionate Principles for the proposition that, "[i]n a world of ever more complex technology, it is increasingly unclear whether the distinction between 'meta-data' and other information carries much weight."[15]

22. When conducted on a massive scale, metadata surveillance deters individuals and groups from exercising their human rights to association and expression. PCLOB made the point that, "bulk collection of telephone records can be expected to have a chilling effect on the free exercise of speech and association, because individuals and groups engaged in sensitive or controversial work have less reason to trust in the confidentiality of their relationships as revealed by their calling patterns."

23. Access asserts that distinguishing information by type is an antiquated way of determining whether it deserves protection. According to the Necessary and Proportionate Principles, "all information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public, should be considered to be 'protected information,' and should accordingly be given the highest protection in law."

24. Communications metadata reveals personal information. Simply because intelligence agencies now have the capacity to collect digital records on a mass scale does not alter the fundamental right to privacy of the individuals whose records are collected. The PCLOB findings, the Necessary and Proportionate Principles, and their endorsement by hundreds of groups worldwide are evidence of a growing agreement that bulk metadata collection violates human rights and offends democratic principles. Thus, we submit to this inquiry that both content data and metadata reveal personal information that is protected as a fundamental right.

25. The UK has been shown to operate a mass surveillance program named Tempora, which was able to tap directly into fibre-optic cables and store huge volumes of data – including content and browsing data – for up to 30 days.[16] Mass surveillance is always arbitrary, and therefore violates Article 17 of the International Covenant on

[14] http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf (at 12)
[15] http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (at 120)
[16] http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq

Civil and Political Rights,[17] which the United Kingdom has ratified.[18]

26. Neither the content of communications nor communications metadata should ever be subject to mass surveillance, which is arbitrary by design and violates UK human rights commitments. Any laws and regulations maintaining distinctions between content and metadata, or authorizing mass communications surveillance, should be reformed in line with the Necessary and Proportionate Principles.

Proposals for specific changes to specific parts of legislation governing the collection, monitoring and interception of private communications.

27. **Specific legal steps are needed, but require greater public debate.**

28. Transparency reporting is an important measure that both governments and companies can take to inform all stakeholders on the state of surveillance, and to move toward remedying abuses of user privacy. Most major internet companies and several large telecoms are issuing transparency reports, which generally disclose: government requests that affect user privacy, access to information, and freedom of expression, such as orders for user data or content removal; compliance rates; the number of accounts affected; the requesting parties and reasons for the requests; and relevant corporate policies and related information.

29. Commendably, Vodafone recently announced it would begin releasing transparency reports with data on wiretap requests worldwide. Stephen Deadman, Vodafone's Group Privacy Officer and Head of Legal for Privacy, Security and Content Standards, stated, "We want all of our customers worldwide to feel they are at liberty to communicate with each other as they see fit. We want our networks to be big and busy with people who are confident they can communicate with each other freely; anything that inhibits that is very bad for any commercial operator."[19]

30. Vodafone's statement underlines the crucial role that transparency plays in reinforcing user trust in companies, and how that trust translates into greater realization of communication and expression rights.

31. Despite Vodafone's intentions to increase transparency, an article on the

---

[17] http://www.slate.com/articles/technology/future_tense/2013/10/martin_scheinin_u_s_u_k_surveillance_programs_violate_iccpr.html

[18] https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en

[19] http://www.theguardian.com/business/2014/jan/15/vodafone-aims-to-disclose-wiretap-demands

announcement notes the extensive restrictions on disclosure imposed on providers by British law, even compared with countries like Turkey, India, and South Africa. According to the Guardian report,[20] British law currently prevents Vodafone from sharing even general information on wiretapping, as "under the Regulation of Investigatory Powers Act (RIPA), discussing the existence of a warrant is punishable by five years in prison."

32. Thus, one specific legal step to take would be to reform RIPA to allow maximum transparency by recipients of government requests on those warrants and other orders that affect user rights. Specifically, companies should be allowed to disclose the number of requests made for user information, the specific number of users affected by the specific number of requests, the specific authorities issuing the request, the specific number of requests complied with, and the specific laws under which the requests were issued.[21] At the same time, the UK government must strive to increase its own transparency on law enforcement and national security requests.

33. Indeed, Access submits that many more reforms are urgently needed to adequately protect the fundamental rights to privacy, freedom of expression, and access to information of users in the UK and abroad. Once a robust public debate occurs, the government should seek to reform its surveillance laws and policies in line with the Necessary and Proportionate Principles.

34. However, in line with our above statements, we feel that more information is needed from the UK government on its current surveillance practices in order to inform a meaningful review of the laws on point. The necessary reforms cannot and will not take place in an environment of government secrecy on surveillance practices, restrictive laws, and limited public consultations.

35. Access appreciates this opportunity to comment on the Committee's inquiry and looks forward to a robust public debate on these pressing issues. For more information on this submission, please contact: Access Policy Counsel Peter Micek at peter@accessnow.org or +1-646-255-4963.

[20] http://www.theguardian.com/business/2014/jan/15/vodafone-aims-to-disclose-wiretap-demands
[21] These correspond to the demands of the 'We Need To Know Coalition'. See https://www.cdt.org/weneedtoknow