Introduction

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working globally to protect digital rights. With over 26,000 active donors and dues-paying members, EFF represents the interests of technology users around the world in both court cases and broader policy debates surrounding the application of law in the digital age. EFF is particularly concerned with protecting electronic privacy at a time when technological advances have resulted in increased Internet surveillance. EFF has served as counsel or amicus curiae in key cases in the United States, addressing the Internet and electronic surveillance by the U.S. government. See, e.g., Jewel v. National Security Agency, 673 F.3d 902 (9th Cir. 2011) (counsel); United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (amicus).

These suggested amendments come from from our earlier submitted analysis of Part 5 of the Investigatory Powers Bill to the Science and Technology Committee, Human Rights Committee and the Joint Committee on the Bill.

The claim to a right to conduct equipment interference is a novel power with many ramifications for users, technology companies, and society in the UK and abroad. Generally, we see Part 5 to be a disproportionate and intrusive surveillance power with insufficient oversight to prevent misuse. In particular, we are very concerned by the new power described in Clause 111 (and reflected later for bulk acquisition in Part 6, Clause 149), which grants a wide range of authorities the ability to compel communications service providers, broadly defined, to assist in the hacking or mass surveillance of their customers and third parties.

We believe in its current form these Parts are in violation of established human rights law, and should be removed or re-drafted in their entirety. In an attempt to limit the damage of the current language, however, the following amendments are offered. They represent narrow corrections to a small subset of the problems found within Part 5 and 6 that we identified in our previous submissions.

The amendments are intended to address four issues, explained below. The amendments themselves follow the explanatory notes.

Please feel free to contact EFF for clarifications via email, c/o Danny O'Brien <danny@eff.org>

Explanatory Notes

This document contains amendments to Clauses 101, 108, 111, 125, 149, 166 for the following purposes.

1. To match RIPA Clause 49 orders, IPB Clause 111 and Clause 149 orders should be served on the most senior officer of communications service providers (CSPs).

The Investigatory Powers Bill contains an ambiguity around the term “communications service provider” which could be interpreted as meaning the *legal* person offering or providing a communications service (Clause 223, 10(a)), or a *human* person within such an organisation with the ability to control such a service (Clause 223, 10(b)).

Under this definition, individual employees within a communications company might be served with a Clause 211 order (and obliged to comply with the duty not to make unauthorised disclosures in Clause 214), instead of an order being served through corporate channels. Equipment interference mandated without the knowledge of senior executives would undermine internal and external trust, damage corporate governance, and could lead to UK-based subsidiaries or personnel of communication companies being denied access or control to common internal systems.

In the Regulation of Investigatory Powers Bill (2000), a similar risk was resolved with Clause.49 (5-6), which requires that demands for decryption keys be served on senior employees or officers of a company, even if junior employees have access to the same keys.

These amendments to Clauses 111 and 149 apply the RIPA standard to equipment interference and bulk acquisition compliance orders.

2. To allow the Secretary of State and Judicial Commissioners to be informed of compulsory steps placed upon CSPs by the intelligence services.

S.111(1) and (2) places differing constraints on CSP compliance, based on whether the warrant was issued for intelligence purposes (S.91-93) or for law enforcement (S.96). For law enforcement, the Secretary of State (or Scottish Ministers) must approve the steps that the CSP will be compelled to take. The Secretary of State does not need to give his explicit approval for these steps in the case of warrants obtained by the intelligence agencies. There is no requirement for these warrants to contain the steps that will be required from CSPs.

This means that for intelligence equipment interference warrants, there will be no oversight or approval by either the Secretary of State nor the Judicial Commissioners for the compelled behaviour forced upon CSPs by the warrant,.This is an omission from the IPB’s stated “double-lock” safeguards.

This amendments to Clauses 101 and 125 would fix this error, by appending a requirement that such steps be described in equipment interference warrants generally.

3. To include a requirement to restore existing service and remove equipment interference measures conducted under Clause 111.

The Joint Committee noted that the bill made insufficient provision for the restoration of previous functionality (and limits on functionality) after a equipment interference warrant had expired.

These amendment to Clauses 108 and 166 extend the requirement to stop behaviour conducted as part of a warrant to compelled communications service providers, and instructs them to restore existing functionality and remove any changes made as part of the cancelled warrant.

4. To prevent loss of trust in protected or privileged communication service providers.

The Investigatory Powers Bill contains protections for certain materials as required by the European Convention on Human Rights: for instance, legally privileged communications, journalistic sources, and the communications of members of legislatures. The use of communications service providers, when those CSPs are primarily used to convey these materials, to assist with equipment interference undermines trust in the integrity of these materials. For instance, a CSP that provides secure communications for lawyers might be used to install malware on their, or their clients' devices. By reducing the trust in these systems, the IPB would chill these vital forms of expression.

This amendment to Clause 111 excludes from the duty on telecommunications operators all services that are specifically designed for these protected materials.

Text of Amendments

Clause 101, Page 79, Line 20, remove: "and"
Clause 101, Page 79, Line 22, add: ", and
"(c) all steps for giving effect to the warrant that telecommunications operators served with a copy of the warrant under S.111 will be required to take."

Explanation: To allow the Secretary of State and Judicial Commissioners to be informed of compulsory steps placed upon CSPs by the intelligence services. (See explanatory note 2, above)

Clause 108, Page 87, Line 23, after "as soon as possible', **add:**
"and all parties served under S.111 be informed of the cancellation. These parties should stop and revert, so far as is reasonably practicable, steps taken under that section in order to restore previously existing functionality and remove any changes made as part of the cancelled warrant."

Explanation: To include a requirement to restore existing service and remove equipment interference measures conducted under Clause 111. (See explanatory note 3, above.)

Clause 111, Page 89, Line 28, add:
"(8) Notice under this section shall not be given to any officer or employee of a telecommunications operator unless he is a senior officer of the body corporate of that telecommunications operator, or it appears to the person giving the notice that there is no senior officer of the body corporate and (in the case of an employee) no more senior employee of the body corporate to whom it is reasonably practicable to give the notice."

Explanation: To match RIPA Clause 49 orders, IPB Clause 111 and Clause 149 orders should be served on the most senior officer of communications service providers (See explanatory note 1, above,)

Clause 111, Page 89, Line 28, add:
"(9) No duty under this section applies to telecommunications operators whose primary telecommunications service is the creation, management, or storage of:

a) legally privileged communications or content

b) journalistic material, communications or content

c) communications or content created by a member of a relevant legislature as defined in S.94(4)."

Explanation: To prevent loss of trust in protected or privileged communication service providers (See explanatory note 4, above.)

Clause 125, Page 100, Line 7, add:

"(7) all steps for giving effect to the warrant that telecommunications operators served with a copy of the warrant under S.111 will be required to take."

Explanation: To allow the Secretary of State and Judicial Commissioners to be informed of compulsory steps placed upon CSPs by the intelligence services (See explanatory note 2 above.)

Clause 149, Page 117, Line 9, add:

"(7) Notice under this section shall not be given to any officer or employee of a telecommunications operator unless he is a senior officer of the body corporate of that telecommunications operator, or it appears to the person giving the notice that there is no senior officer of the body corporate and (in the case of an employee) no more senior employee of the body corporate to whom it is reasonably practicable to give the notice."

Explanation: To match RIPA Clause 49 orders, IPB Clause 111 and Clause 149 orders should be served on the most senior officer of communications service providers (See explanatory note 1 above,)

Clause 166, Page 129, Line 22, after "*as soon as possible****", add:***

"and all parties served under S.167 (5) be informed of the cancellation. These parties should stop and revert, so far as is reasonably practicable, steps taken under that section in order to restore previously existing functionality and remove any changes made as part of the cancelled warrant.

Explanation: To include a requirement to restore existing service and remove equipment interference measures conducted under Clause 111. (See explanatory note 3 above.)