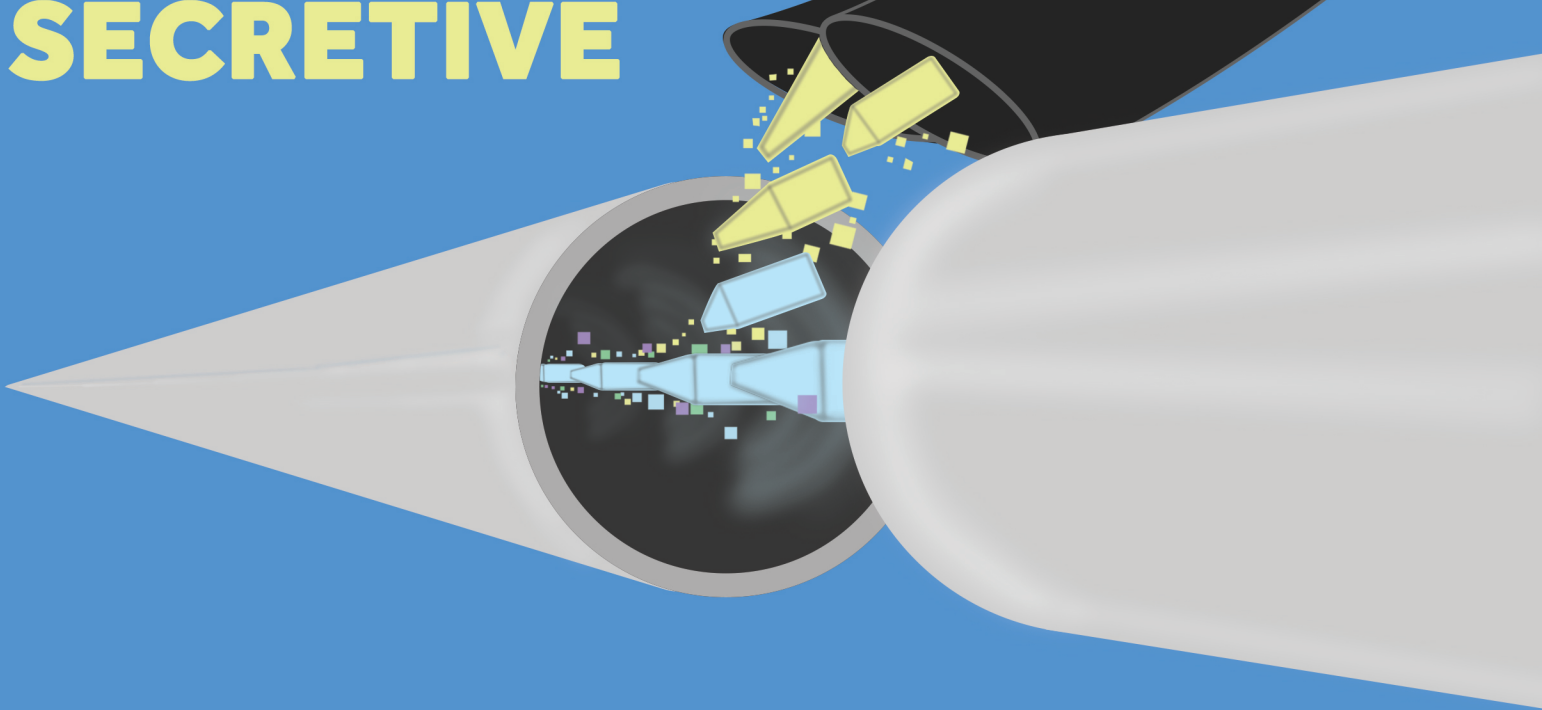


# NOT A SECRET:

BULK INTERCEPTION PRACTICES  
OF INTELLIGENCE AGENCIES



AS EUROPEAN GOVERNMENTS OPENLY  
DISCUSS BULK CABLE INTERCEPTION,  
**THE U.S. REMAINS  
UNNECESSARILY  
SECRETIVE**



SEPTEMBER 2019

## Contents

<b>Methodology</b>	1
<b>Executive Summary</b>	2
<i>Box - US Bulk Cable Interception Practices</i>	4
<b>Intercepting the International Cable Network</b>	5
<i>Conceptual Model of Signals Intelligence</i>	6
<i>Signal - the International Cable Network [CCM - 1]</i>	7
<i>Slide - NSA Explanation of Targeting Within a Fiber Optic Cable</i>	9
<i>Photographs - U.K. Cable Landing Points</i>	10
<i>Collection - Intercepting Cable Traffic [CCM - 2]</i>	12
<i>Extraction</i>	12
<i>Filtering</i>	13
<i>Storage, Analysis and Dissemination</i>	14
<b>United Kingdom</b>	14
<i>Background</i>	15
<i>Official Confirmation</i>	16
<i>Box - Big Brother Watch v U.K.</i>	17
<i>Legal Regime</i>	18
<i>Bulk Collection in Practice</i>	20
<i>Collection</i>	20
<i>Filtering</i>	22
<i>Filtering Internal U.K. Communications</i>	22
<i>Selection for Examination</i>	22
<i>Examination</i>	25
<i>Conclusion</i>	25
<b>Sweden</b>	26
<b>Germany</b>	29
<b>The Netherlands</b>	32
<b>Finland</b>	34
<b>Other Countries</b>	35
<b>Conclusion</b>	38
<i>Annex I - Acronyms</i>	40
<i>Annex II - Legislation</i>	40

## Methodology

*This report by the Center for Democracy & Technology (CDT) was authored by London-based surveillance expert Eric Kind and edited by CDT's Greg Nojeim. It was made possible by a grant from the Open Society Foundations.*

This report primarily relies on officially released material from a variety of sources including legislation and accompanying explanatory documents, oversight reports, legal submissions, government-initiated independent reviews, and on-the-record media interviews. A number of interviews helped provide background to documents in foreign languages.

The author is grateful for the assistance of Mathias Vermulean, Veremat; Thorsten Wetzling, Kilian Vieth, Stiftung Neue Verantwortung; Fredrik Bergman, Alexander Ottosson, Centrum for Rattvisa; Félix Tréguer, Science Po; Hans de Zwart, Lotte Houwing, Bits of Freedom; Caroline Wilson Palow, Privacy International; Megan Goulding, Liberty; Tamir Israel, CIPPIC; Martin Scheinin, European University Institute; and Erka Koivunen, F-Secure. In each case, organizations are listed for purposes of identification only. CDT's Joseph Lorenzo Hall, Chris Calabrese, and Mana Azarmi also provided helpful comments.

**NOT A SECRET**

## *Executive Summary*

In the United States, the government takes the position that bulk cable interception is a state secret — so secret that litigation challenging its lawfulness and compliance with the U.S. Constitution cannot proceed without revealing information that would pose a grave risk to U.S. national security.<sup>1</sup>

Yet bulk cable interception is an officially confirmed practice in a number of countries around the world. The governments of the United Kingdom, Sweden, Germany, the Netherlands, Finland, France, and Canada have all officially confirmed that they undertake bulk cable interception. Other countries like Norway are also in the process of legislating for the practice.

In these countries, bulk cable interception is not a secret. Instead the practice is set out in legislation and accompanying explanatory documents, it is reviewed and publicly reported on in oversight reports and government-initiated independent reviews, and discussed in on-the-record media interviews.

Officials in a number of countries have set out the key stages for bulk cable interception, clearly linking the legal framework to the technical processes. In the U.K., officials have acknowledged a four-stage process, covering collection, filtering, automated selection, and human examination. In Sweden, they have set out a six-stage process of collection, automatic selection, data processing, analysis, dissemination, and feedback. In the Netherlands, officials have set out a four-stage process of preparation, data collection, processing, and analysis, with many sub-stages including cable selection, filtering, and data enrichment.

Oversight bodies of different countries have undertaken detailed scrutiny of bulk cable interception, including at the selector level. Between 2010 and 2014, the Swedish oversight body audited the Swedish intelligence agencies' use of selectors on 17 occasions; the Dutch oversight body is currently reviewing whether selectors are sufficiently targeted and relevant to investigative priorities.

Detailed technical discussion has taken place around the challenge of filtering out communications of a country's own citizens or residents. In Sweden, oversight reports include a discussion of the difficulty in separating domestic cable-based communications from those crossing the Swedish border, and the steps the Swedish intelligence agency has taken to address that problem, such as separating communications manually at the processing or analyzing stage. In Germany, a three-stage technical filtering process has been officially disclosed, along with the number of selection terms intelligence officials are seeking to filter out, and the number of selectors used to filter out known German nationals who are abroad.

Some countries, such as Sweden undertook significant public debates before their intelligence agencies began the practice, and Norway is in the midst of such debate now. When the U.K. overhauled the legal

---

<sup>1</sup> See Jewel v NSA: <https://www.eff.org/cases/jewel>.

framework for bulk interception after the Snowden revelations, it published an “operational case” seeking to establish the need for bulk cable interception, and it commissioned independent reviews to assess and report publicly on whether the operational case was adequate.

There have been legal cases brought against the practice in the Netherlands, Sweden, Germany, and the U.K., and in each case, a court heard the challenge. Governments defending the challenged practices officially confirmed bulk interception capabilities. In the case of the U.K., the courts have even confirmed the identities of non-profit groups whose communications were unlawfully retained and selected under bulk interception programs run by U.K. intelligence agencies.

This relatively open discussion of bulk cable interception in Europe contrasts sharply with the efforts of the U.S. government to shield it from public scrutiny by citing the state secrets privilege. It calls into question the assertion by the U.S. government that the practice cannot be discussed in U.S. courts for fear of disclosing information that would pose a grave risk to U.S. national security.

The focus of this report is transparency about the technical efforts of governments worldwide to undertake bulk cable interception. It is not intended to be an analysis of the legal framework in these countries, instead focusing on the practice, and only drawing on the legal framework where helpful to understand that practice. While the countries analyzed here should be applauded for the transparency they have been able to achieve, official confirmation has had its limits and transparency can and should go further than it has thus far.

The report first sets out how the international cable network operates, and how communications that traverse it can be intercepted, with reference to a conceptual model of signals intelligence, explaining the process of extraction, filtering, storage, and analysis.

The report then undertakes a detailed analysis of the U.K. practice of bulk cable interception. It considers the historical background to bulk cable interception, the legal regime underpinning modern day practice, and recounts chronologically the U.K.’s gradual official confirmation of its bulk cable interception capabilities. Analysis of the official confirmed bulk interception process is then undertaken, reviewing how the U.K. system undertakes bearer selection, filtering, automatic selection for examination, and examination by human analysts.

Finally, a high-level review is provided of the bulk cable interception practices of Sweden, Germany, the Netherlands, Finland, France, Canada, South Africa, and Norway, highlighting specific officially-confirmed efforts that are unique to each country.

In setting out how transparent other countries are able to be in both the law governing bulk cable collection and the technical practice, this report seeks to counter the assertion that similar levels of transparency in the U.S. would amount to a grave risk to U.S. national security. Excessive secrecy is

thwarting public debate about whether to permit bulk cable interception at all, and whether efforts to outlaw the practice of bulk collection domestically<sup>2</sup> have been effective.

The United States has confirmed little with regard to its own bulk cable collection practices. In Presidential Policy Directive 28,<sup>3</sup> the U.S. acknowledged that it engages in bulk collection, but did not specify how collection was undertaken. PPD-28 did not impose substantial limitations on such collection. It did articulate six broad uses to which information collected in bulk could be put, and indicated that the President could contract or expand that list. A subsequent report by the Privacy and Civil Liberties Oversight Board (PCLOB) indicated that as a practical matter, the PPD-28 use limitations were already in effect prior to issuance of PPD-28.<sup>4</sup>

In addition, in a July 2, 2014 report, PCLOB described an Upstream collection program conducted pursuant to Section 702 of the Foreign Intelligence Surveillance Act.<sup>5</sup> Upstream collection of internet communications involves the compelled assistance of communications service providers who operate the “internet backbone” in the U.S. The U.S. government regards Upstream as a targeted, as opposed to a bulk collection program, but this is matter of some contention as indicated in the *Jewel v. NSA* litigation.<sup>6</sup> The U.S. has revealed very little information about how the surveillance program is conducted, but has described in vague terms the selectors that can be used to identify communications, and that communications collected can be “to,” “from,” or “about” a selector. The NSA abandoned “abouts” collection in 2017 because it could not be conducted lawfully given current technology.<sup>7</sup>

After it was disclosed in June of 2013 by former NSA contractor Edward Snowden, the U.S. acknowledged that it was collecting in bulk records of phone calls to, from, and within the United States. Two years after it was disclosed, Congress outlawed the bulk collection of telephony metadata in the USA FREEDOM Act and substituted it for a broad, but targeted, program for collection of call detail records.

Snowden revealed five bulk collection programs that the U.S. government has thus far declined to confirm, and about which it has revealed little to no information: DISHFIRE, CO-TRAVELER,

---

<sup>2</sup> See, e.g., the USA FREEDOM Act, Pub. L 114-23 (2015), Section 103, 201 and 501.

<sup>3</sup> Presidential Policy Directive – Signals Intelligence Activities (PPD-28), (Jan. 17, 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

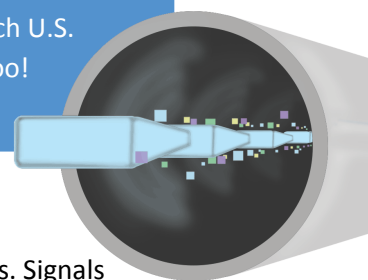
<sup>4</sup> Presidential Policy Directive 28 (PPD-28) Report, 6, *Privacy and Civil Liberties Oversight Board*, (Oct. 16, 2018), <https://www.pclob.gov/reports/report-PPD28/>.

<sup>5</sup> Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, pp. 35-40, *Privacy and Civil Liberties Oversight Board*, (July 2, 2014), <https://www.pclob.gov/library/702-Report.pdf>.

<sup>6</sup> See, Electronic Frontier Foundation landing page on *Jewel v. NSA*, <https://www.eff.org/cases/jewel>.

<sup>7</sup> NSA Stops Certain Section 702 “Upstream” Activities, Release No: PA-014-18, (April 28, 2017), <https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/>.

MUSCULAR, MYSTIC, and QUANTUM.<sup>8</sup> Cell site location information, text messages, call detail records, and other information are collected. The MUSCULAR program, through which U.S. intelligence authorities collected in bulk traffic that flowed between Google and Yahoo! data centers, reportedly involved bulk cable interception techniques.<sup>9</sup>



## *Intercepting the International Cable Network*

This report deals with the practice of bulk cable interception by signal intelligence agencies. Signals intelligence is the means and methods for intercepting and analyzing electronic signals, including radio, satellite, and cable-bound communications. Signals intelligence agencies like the U.S. National Security Agency (NSA), the U.K. Government Communications Headquarters (GCHQ), the German Federal Intelligence Service (BND), and the Swedish National Defense Radio Establishment (FRA) collect communications using these methods to analyze them in accordance with the national laws, for purposes like protecting national security.

Traditionally, signals intelligence agencies collected information using masts and dishes to intercept radio or satellite signals. Today, the majority of the information that interests intelligence agencies flows through the international cable network, and thus bulk cable interception can be the main source of intelligence for modern day signals intelligence agencies.

There are a number of different terms to describe such collection practices, each with contested definitions. Terms like mass surveillance, bulk collection, and targeted or untargeted interception all have different meanings to different stakeholders in different countries, and there isn't yet a common lexicon. This report will use the terms bulk collection and bulk interception interchangeably, following the loose definition provided by the U.S. National Academy of Sciences.<sup>10</sup>

This section of the report will introduce a conceptual model of signals intelligence to act as a guide in considering national frameworks. It will explain the technical details of how the international cable network operates, and then how communications are extracted, filtered, stored, and analyzed by signals intelligence agencies. The purpose of this section is to provide the conceptual and technical grounding

---

<sup>8</sup> Secret Surveillance: Five Large-Scale Global Programs, A Joint Submission of CDT and ACLU to the UN Human Rights Council in connection with the Universal Periodic Review of human rights practices of the U.S. in May, 2015, <https://cdt.org/files/2014/09/cdt-aclu-upr-9152014.pdf>.

<sup>9</sup> NSA Infiltrates links to Yahoo, Google centers worldwide, Snowden Documents say, *The Washington Post*, (Oct. 30, 2013), [https://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](https://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).

<sup>10</sup> "If a significant portion of the data collected is not associated with current targets, it is bulk collection; otherwise, it is targeted. There is no precise definition of bulk collection, but rather a continuum, with no bright line separating bulk from targeted. The committee acknowledges that use of the word "significant" makes its definition imprecise as well." Summary, Bulk Collection of Signals Intelligence: Technical Options, National Academy of Sciences (2015) available at: <http://nap.edu/19414>.

for the rest of the report, and act as a reference point as the practices of different countries are analyzed.

### *Conceptual Model of Signals Intelligence*

A slightly adjusted conceptual model for signals intelligence provided by the U.S. National Academy of Sciences<sup>11</sup> will be used as a reference throughout this report for understanding the key steps in the signals intelligence process. This conceptual model has been selected because it is primarily technical in nature, and does not carry with it the marks of any particular legal framework, nor language that, while precise, may be considered contentious.

The diagram (Fig. 1) is provided by the U.S. National Academy of Sciences and sets out the interception of signals, the extraction of data, subsequent filtering including by discriminants such as selectors, before it is stored, queried, analyzed, and packed into intelligence reports. This report's primary focus is the 'collection' phase. This report uses the high level conceptual stages in that diagram, but tailors the sub-stages and description of each stage to bulk cable interception.

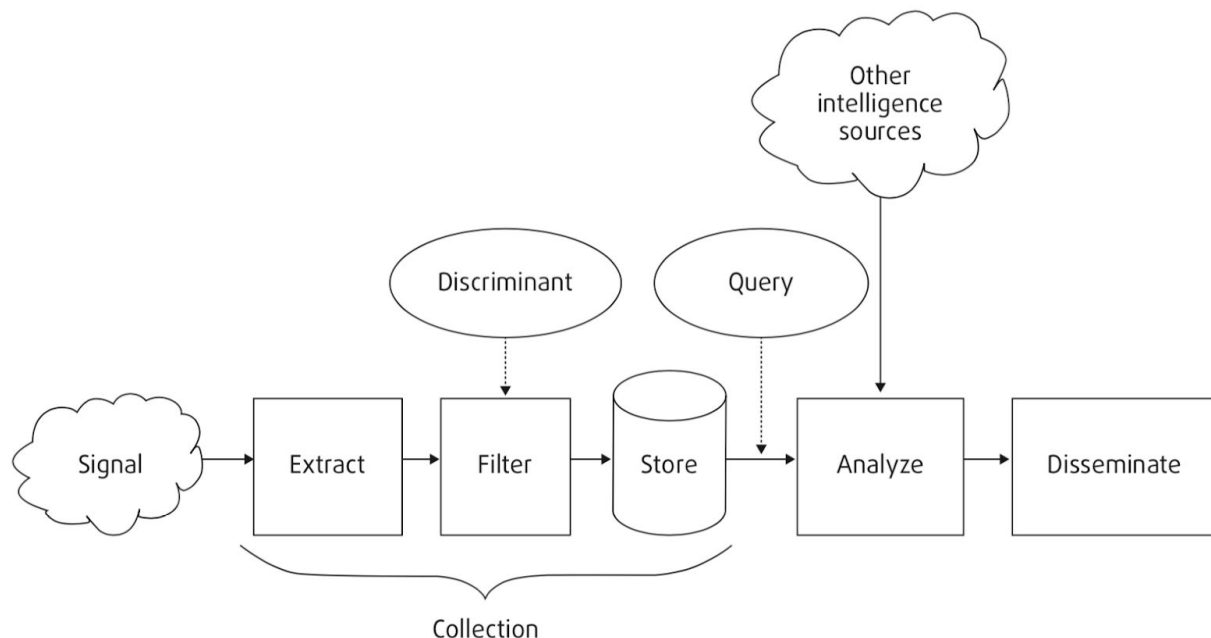


Fig. 1: *Bulk Collection of Signals Intelligence: Technical Options, National Academy of Sciences* (2015)

#### **Core Conceptual Model (CCM)**

1. **Signal:** Communications are transmitted via fiber optic cables which span the globe
2. **Collection:** The extraction, filtering, and storing of data.

<sup>11</sup> Bulk Collection of Signals Intelligence: Technical Options, National Academy of Sciences (2015) available at: <https://www.nap.edu/catalog/19414/bulk-collection-of-signals-intelligence-technical-options>.



- a. **Extract:** To acquire communications, physical probes<sup>12</sup> are placed on cables to intercept communications carried on bearers (channels in a cable fiber).<sup>13</sup>
    - i. Probes are placed on cables,
    - ii. Bearerers are selected for capture, and
    - iii. Communications are subjected to subsequent processing.
  - b. **Filter:** To reduce the volume of material, further processing is undertaken commonly using a discriminant to set out what should be discarded and what should be retained.
    - i. "Negative filters" can be used to remove certain types of traffic.
    - ii. "Positive filters" such as selectors relating to targets can be used to identify communications of intelligence value.
  - c. **Store:** Material is stored for future use.<sup>14</sup>
3. **Analyze:** Human analysts review material, searching databases with different types of queries, and combining the material with intelligence with other sources.
  4. **Disseminate:** Finalized intelligence reports are shared with government customers and other intelligence agencies.

There are a number of different ways such a model could be represented, with this Core Conceptual Model being a reasonably simplistic rendering. Different countries and different intelligence agencies have different ways of conceptualizing the signals intelligence, and use different words to describe different parts of the model. Even within a single country, there can be different words to describe the same activity, depending on whether it is being approached technically, legally, or as a question of policy. For the purpose of this report, different countries' frameworks will be represented as they are found, but reference will be made to this Core Conceptual Model using square brackets e.g. [CCM - 2.a.i] at key points so comparisons can be made.

### *Signal – the International Cable Network*

The vast majority of internet communications are carried around the world with high-capacity fiber optic cables, often laid on the sea bed or underground. It is these cables that are the focus of bulk interception efforts.

---

<sup>12</sup> A probe is equipment installed on a fiber network segment that can act as an "optical router," allowing for changing, duplication, and modification of light paths as data flows across the fiber pairs making up the segment. This allows for capturing and copying of traffic flows, in addition to network management. See: [https://sii.transparencytoolkit.org/docs/Glimmerglass\\_Intelligent-Optical-System\\_Product-Description\\_1sii\\_documents](https://sii.transparencytoolkit.org/docs/Glimmerglass_Intelligent-Optical-System_Product-Description_1sii_documents).

<sup>13</sup> Data is transmitted through fiber optic cables as light. By transmitting light at different frequencies using a variety of different methods a cable is able to carry a number of different bearers. "Bearer" is a term used in this context to describe the separate channels into which a fiber's capacity is divided; each channel can contain many individual communications sessions (depending on the type of communication and the relative bandwidth needed).

<sup>14</sup> More complicated models would represent the fact that once stored, data matching certain criteria is further processed to assist with future analysis, perhaps by summarizing the content of voice calls, deploying voice or gender identification tools to audio intercepts, or extracting events from the content of emails.

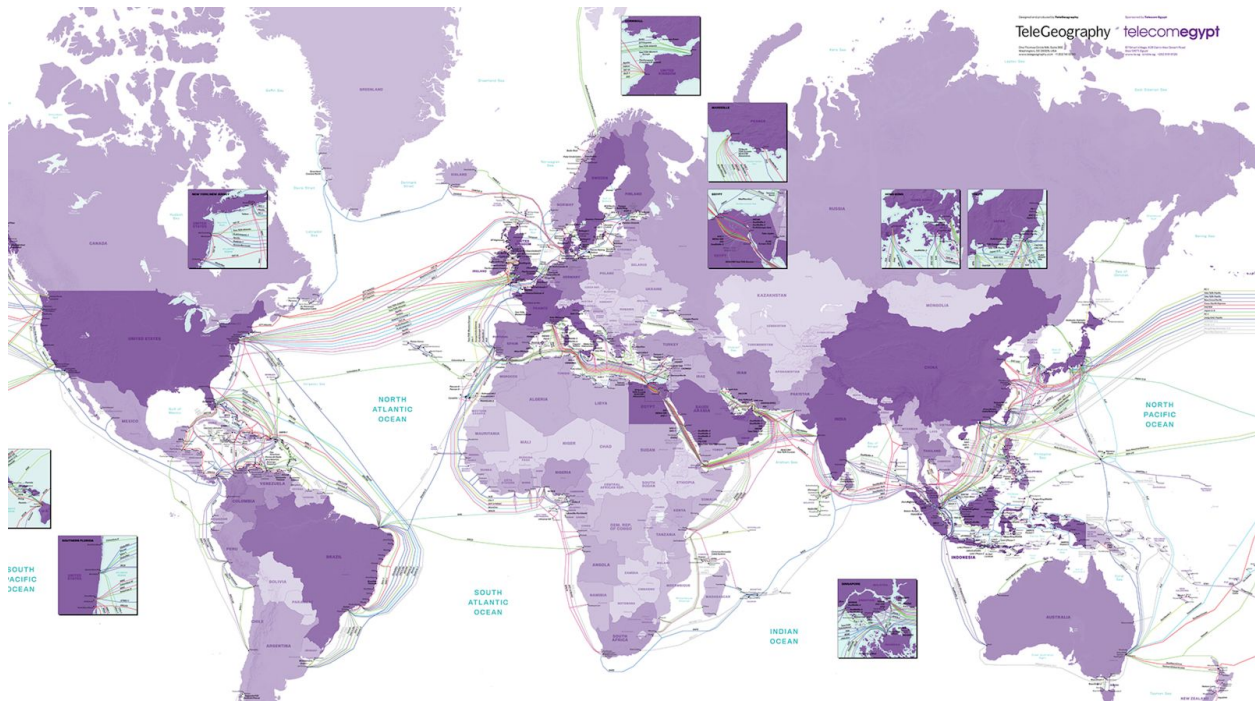


Fig. 2: [Tele-geography Submarine Cable Map](https://www.submarinecablemap.com/)

The map (Fig. 2) shows the international cable network.<sup>15</sup> The ownership, length of cable, landing points, and capability of each cable is all public information and aggregated by a number of different companies.<sup>16</sup> For example FLAG Europe Asia<sup>17</sup> is a primarily underwater cable with a capacity of 10Gbps, a length of 27000 km and with landing points in Alexandria, Egypt; Aqaba, Jordan; Estepona, Spain; Fujairah, United Arab Emirates; Jeddah, Saudi Arabia; Keoje, Korea; Lantau Island, Hong Kong, China; Miura, Japan; Mumbai, India; Palermo, Italy; Penang, Malaysia; Porthcurno, United Kingdom; Satun, Thailand; Shanghai, China; Songkhla, Thailand; and Suez, Egypt.

Data is transmitted through fiber optic cables as light. By transmitting light at different frequencies using a variety of different methods, a cable is able to carry a number of different "bearers." "Bearer" is a term used in this context to describe the separate channels into which a fiber's capacity is divided.

<sup>15</sup> Tele-geography Submarine Cable Map, <https://www.submarinecablemap.com/>.

<sup>16</sup> See Tele-geography <https://www.submarinecablemap.com/>; Infrapedia <https://live.infrapedia.com> and Greg's Cable Map <https://cablemap.info/default.aspx>.

<sup>17</sup> FLAG, Tele-geography, available at: <https://www.submarinecablemap.com/#/submarine-cable/flag-europe-asia-fea>.

GCHQ has described<sup>18</sup> that “[i]n one transatlantic cable for example, there are eight fibers (arranged as four pairs). These are used in a way that allows them to carry 47 separate bearers, each operating at 10 [gigabits per second (‘giga-’ means one thousand million, and ‘bit’ means binary digit)].”

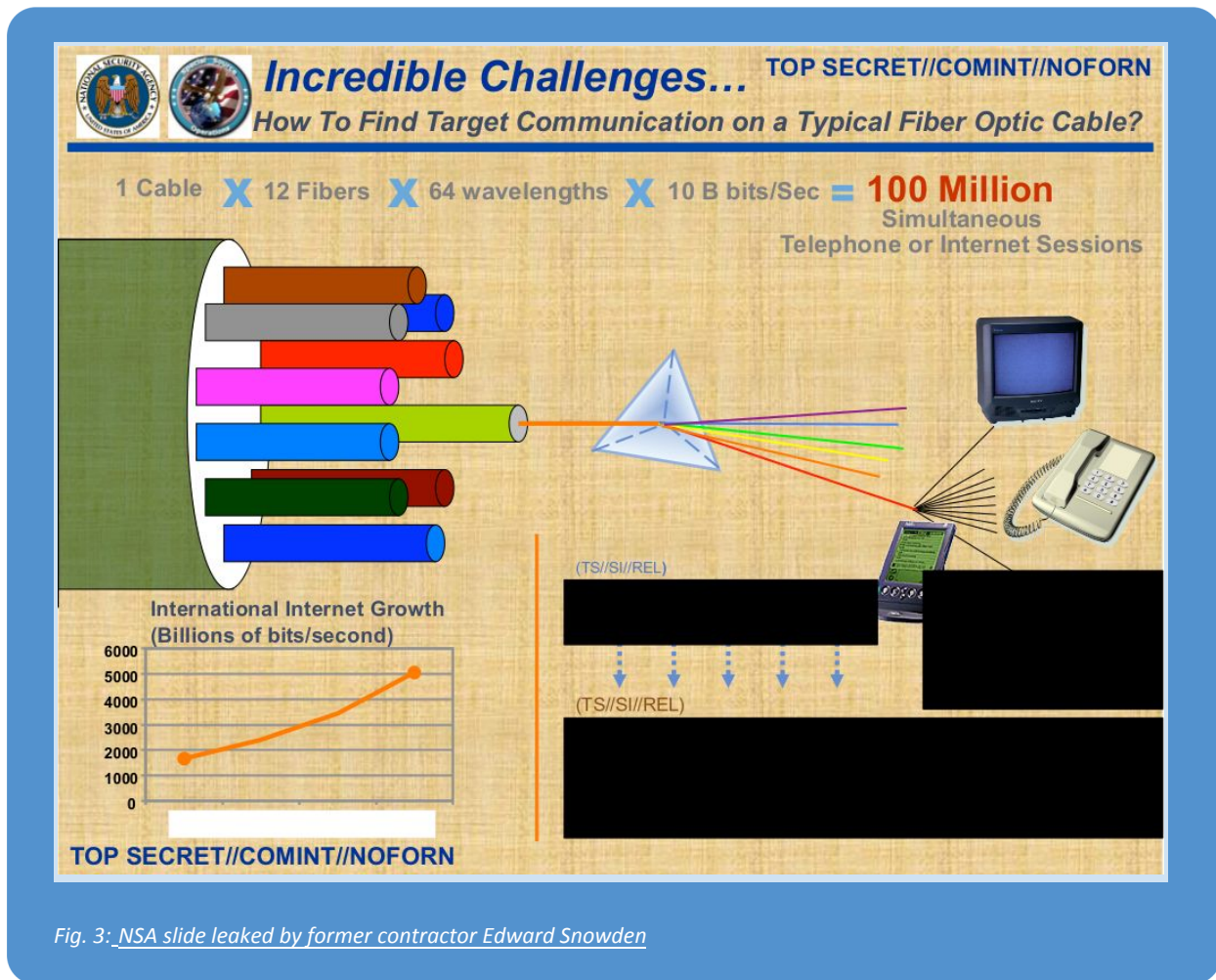


Fig. 3: NSA slide leaked by former contractor Edward Snowden

<sup>18</sup> “GCHQ explained that the internet is carried on physical cables that are laid on the sea bed or underground: “These are quite big (typically 69mm in diameter, or about as thick as your wrist) and heavy (10 kg per metre). They are made up of a series of layers (polyethylene on the outside, mylar tape and stranded steel wire to provide strength, aluminium to keep out water and polycarbonate to protect the heart of the cable, which consists of a copper tube filled with petroleum jelly in which sit a small number of optical fibers). These fibers carry the data. In one transatlantic cable for example, there are eight fibers (arranged as four pairs). These are used in a way that allows them to carry 47 separate bearers, each operating at 10 [gigabits per second (‘giga-’ means one thousand million, and ‘bit’ means binary digit)]. You could think of these bearers as analogous to different television channels – there are various ways of feeding multiple bearers down a single optical fiber, with the commonest being to use light of different frequencies. Technology is evolving fast, and there are cables planned for the near future which will contain six pairs of optical fibers, each capable of handling 100 bearers operating at 100 [gigabits per second]”” ‘Privacy and Security: A modern and transparent legal framework’, The Intelligence and Security Committee of Parliament (2013) available at: [https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312\\_ISC\\_P%2BS%2BRpt%28web%29.pdf](https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf).

This leaked NSA slide from 2010,<sup>19</sup> shows the fiber-optic cable, the individual fibers within the cable, and the wavelengths transmitted within each fiber and the capacity of each. The diagram shows a prism refracting out different frequencies of light represented as different colors. Each wavelength contains the communications from mobile devices and phones.

The U.K. government has asserted that there are approximately 100,000 bearers that make up the global internet.<sup>20</sup> The capacity of these cables is not static, but rather is increasing as technology advances. GCHQ has explained that in the near future there will be cables “which will contain six pairs of optical fibers, each capable of handling 100 bearers operating at 100 [gigabits per second].”<sup>21</sup>

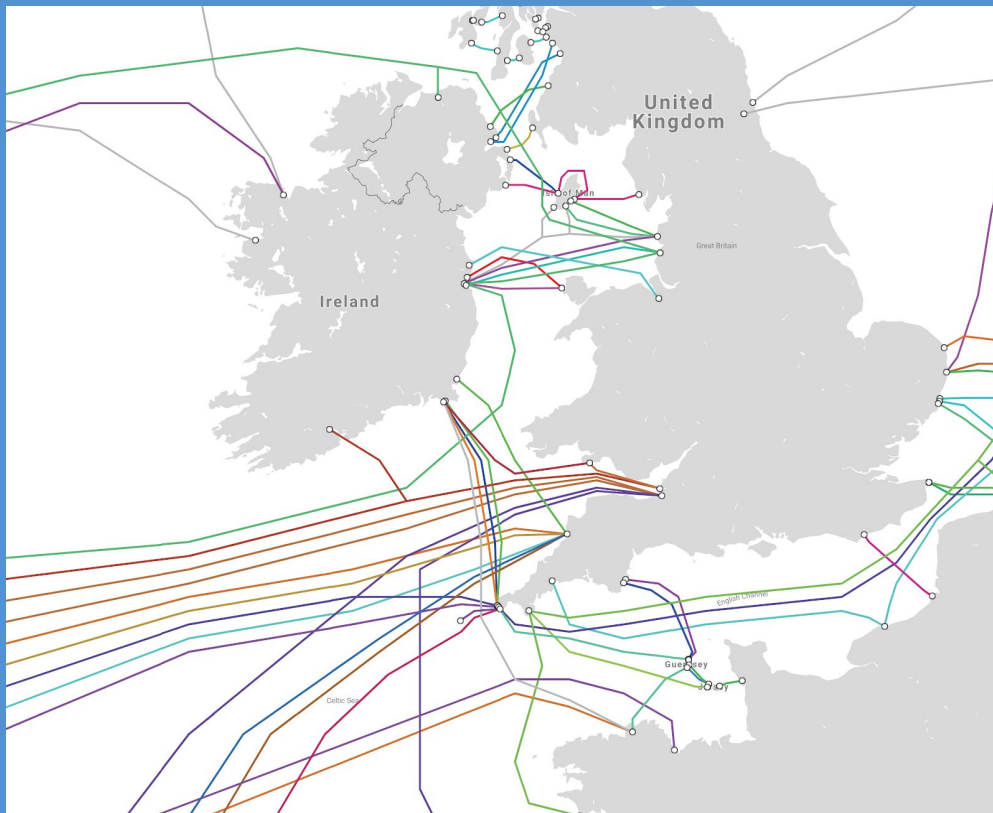


Fig. 4: Tele-geography Submarine Cable Map<sup>22</sup>

<sup>19</sup> This slide was among the documents leaked by former NSA contractor Edward Snowden and it can be found at <https://cryptome.org/2014/06/nsa-information-intercept-14-0619.pdf>, p. 36.

<sup>20</sup> Privacy and Security: A modern and transparent legal framework', The Intelligence and Security Committee of Parliament (2013) available at: [https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312\\_ISC\\_P%2BS%2BRpt%28web%29.pdf](https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf).

<sup>21</sup> Privacy and Security: A modern and transparent legal framework', The Intelligence and Security Committee of Parliament (2013) available at: [https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312\\_ISC\\_P%2BS%2BRpt%28web%29.pdf](https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf).

<sup>22</sup>Tele-geography Submarine Cable Map, <https://www.submarinecablemap.com>.





Fig. 5: Screenshot from "The Secrets Of Cornwall - Part 1 - Communications"<sup>23</sup>



Fig. 6: Screenshot from "The Secrets Of Cornwall - Part 1 - Communications"<sup>24</sup>

<sup>23</sup> Screenshot from 'The Secrets Of Cornwall - Part 1 - Communications', Mark Thomas (2016) available at: [https://www.youtube.com/watch?v=K\\_nnUbX7uuQ](https://www.youtube.com/watch?v=K_nnUbX7uuQ).

<sup>24</sup> Screenshot from 'The Secrets Of Cornwall - Part 1 - Communications', Mark Thomas (2016) available at: [https://www.youtube.com/watch?v=K\\_nnUbX7uuQ](https://www.youtube.com/watch?v=K_nnUbX7uuQ).

### Collection - Intercepting Cable Traffic

It is not possible to extract specified communications, or particular communications to or from a specified identifier, from the bearer.<sup>25</sup> Instead, in the bulk cable interception context, all the communications on the bearer have to be collected in a single act of interception.

When a communication, such as an email, is sent over the internet, it is broken down into separate components or “packets” that are transmitted separately, possibly via different routes, until it reaches the recipient where it is reassembled.<sup>26</sup> Governments have argued this is why it’s important to collect in bulk from a number of cables to ensure they are able to piece all the packets together, although in practice packets will often follow the same route thus a complete communication is often able to be captured from within a single bearer.

The U.K. government has provided a practical example:<sup>27</sup>

*[I]f an intercepting agency needs (for example) to obtain communications sent to an individual (C) in Syria, whilst they are being transmitted over the internet, and has access to a given bearer down which such communications may travel, the intercepting agency will need to intercept all communications that are being transmitted over that bearer – at least for a short time – in order to discover whether any are intended for C.*

*Further, since the packets associated with a given communication may take different routes to reach their common destination, it may be necessary to intercept all communications over more than one bearer to maximise the chance of identifying and obtaining the communications being sent to C.*

### Extraction

To collect and extract information from a cable, a physical probe [CCM 2.a.i] is placed on it. A number of different companies produce such probes<sup>28</sup> and it is likely that agencies will also develop their own custom hardware. A picture of the probe created by Glimmerglass is pictured in Fig. 7. Probes provide theoretical access to communications that pass through the cables, but it is only once individual bearers within the cable are identified and selected for collection [CCM 2.a.ii] that communications are intercepted.

---

<sup>25</sup> See “for technical reasons, it is necessary to intercept the entire contents of a fibre optic cable (or “bearer”) in order to obtain any intercepted communications or communications data from it at all.” United Kingdom’s Observations on the Grand Chamber’s Questions to the Parties (3 May 2019).

<sup>26</sup> ‘Operational case for Bulk Powers’, U.K. Government, (2016), available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/504187/Operational\\_Case\\_for\\_Bulk\\_Powers.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf).

<sup>27</sup> United Kingdom’s Observations on the Grand Chamber’s Questions to the Parties’, Big Brother Watch v U.K. Application No. 58170/13, §16, (May 2019) available at: <https://privacyinternational.org/sites/default/files/2019-07/UK%20Gov%20Obs%20-%20Revised%20Version%20-%20May%202019.PDF> [hereinafter referred to as U.K. Observations, May 2019].

<sup>28</sup> ‘Surveillance Industry Index’, Privacy International, available at: [https://sii.transparencytoolkit.org/search?product\\_facet=International+Gateway](https://sii.transparencytoolkit.org/search?product_facet=International+Gateway).

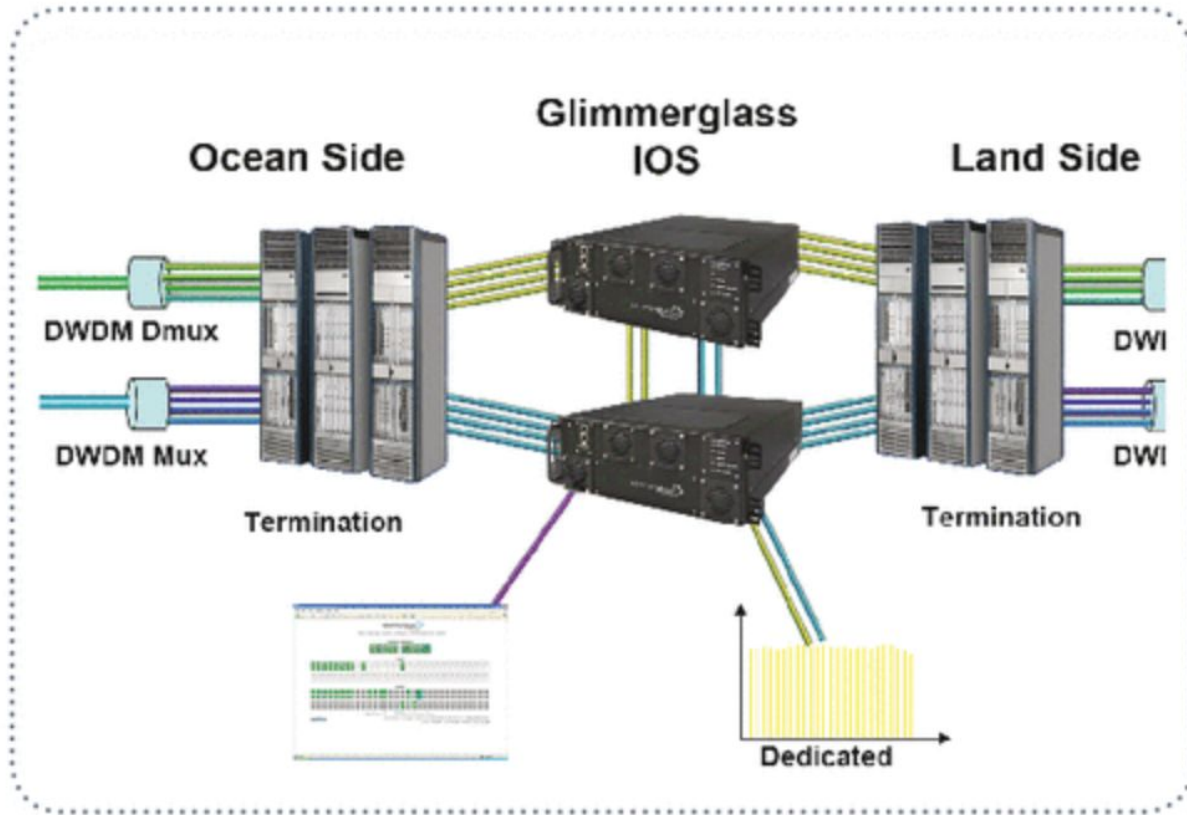


Fig. 7: [Glimmerglass company document picturing a physical probe.](#)

Some countries, including the U.K., refer to the practice of bearer selection [CCM 2.a.i] openly in oversight reports, in court submissions, as well as in legislative Codes of Practice.<sup>29</sup>

### Filtering

The quantity of material that a bearer transmits is significant. In order to restrict interception to relevant material, a number of steps are taken to try and reduce the quantity obtained. This process is different in each country and undertaken for both technical and legal reasons. Often a discriminant is used to help to set out what should be discarded and what should be retained.

1. Negative filters are used to identify material to discard, such as high bandwidth traffic like video streaming services (e.g. Netflix is likely to contain little of intelligence value and so would be discarded at the earliest possible opportunity).
2. Positive filters are used to identify material to retain. Commonly this would be the deployment of selectors (e.g. email address or phone number) from a targeting database.

<sup>29</sup> In the U.K. context, a Code of Practice is a statutory instrument, approved by Parliament, which is used to provide practical measures that enable the law to be enforced and operate in daily life. Codes are legally binding and take primacy over any internal advice or guidance.

Many European countries that are undertaking bulk cable interception have legal rules that require them to filter out the communications of their nationals. Germany's BND uses a number of positive and negative filters in conjunction as part of its DAFIS filter system designed to ensure that German nationals' communications are omitted from their bulk interception systems.<sup>30</sup>

This step is also the primary method by which agencies begin targeting specific communications with selectors as part of the positive filter.

### *Storage, Analysis, and Dissemination*

Communications are then stored for consideration by human analysts, who will combine the material with intelligence from other sources. Intelligence reports will be produced from the material, which will be shared with government customers and other intelligence agencies.

Different countries have different legal frameworks governing how long data can be retained for.

## *United Kingdom*

In the last five years, the U.K. has shifted its stance on public avowals of bulk interception practices dramatically, going from blanket secrecy about bulk interception to adopting a comprehensive approach to official confirmation that demonstrates world-leading transparency.

Today, bulk cable interception is officially confirmed and there is detailed statutory language governing the practice in the *Investigatory Powers Act 2016*. The government published fact sheets to help the public understand the practice. An operational case for all the bulk powers in the *Investigatory Powers Act 2016* was also published by the government<sup>31</sup> and an independent review of the operational case<sup>32</sup> was undertaken by a team led by the then-Independent Reviewer of Terrorism Legislation, Lord Anderson of Ipswich KBE QC.<sup>33</sup> There are detailed technical explanations of the practice provided by the government, covering how intelligence agencies identify bearers to intercept, how they filter and select communications, and how they subsequently use the collected information. There have even been

---

<sup>30</sup> See "Germany" section of this report.

<sup>31</sup> 'Operational case for Bulk Powers', U.K. Government, (2016), available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/504187/Operational\\_Case\\_for\\_Bulk\\_Powers.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf).

<sup>32</sup> 'Independent review of the operational case for bulk powers: Terms of Reference', U.K. Parliament, (2016), available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/527764/TOR\\_for\\_Bulk\\_Review.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/527764/TOR_for_Bulk_Review.pdf).

<sup>33</sup> The Independent Reviewer of Terrorism Legislation is appointed by the U.K. government to review anti-terrorism law in the United Kingdom and issue regular reports for the Home Secretary or Treasury before being laid in Parliament. Lord Anderson of Ipswich KBE QC is a senior barrister, who was the Independent Reviewer from 2011-2017 and undertook a number of key reviews relating to U.K. surveillance powers. He is now a member of the House of Lords and was honored by the Queen for his services to national security and civil liberties.



judicial findings which confirmed that two non-governmental organizations, Amnesty International and the South African Legal Resources Center, were subjected to unlawful bulk interception practices.

This section will briefly cover the history of bulk interception in the U.K., before reviewing how the U.K. came to officially confirm the modern day practice. Analysis will be provided of the legal regime as it stands today, and how the U.K. bulk collection program functions in practice from bearer selection through to filtering, selection for examination, and finally examination by a human analyst.

### Background

There has been a long history in the United Kingdom of the state gaining access to telecommunications cables in bulk for the purpose of surveillance.<sup>34</sup> The first legislative provision in the U.K. governing the large scale interception of communications was Section 4 of the *Official Secrets Act 1920*. It permitted the Secretary of State to issue a warrant to be served on telegraph operators to acquire the entirety of telegrams entering or leaving the country.<sup>35</sup> The use of the power lay unscrutinized other than a passing mention in The Radcliffe Report on the D-Notice affair, which confirmed that the power “does involve a regular collection of copies of messages transmitted by the Post Office and other cable offices with a view to the total collected being sorted and certain defined categories of them being set aside for inspection by the intelligence agents of Her Majesty’s Government.”<sup>36</sup> The Act lasted until 1985, when the relevant sections were ultimately updated and extended within the *Interception of Communications Act 1985*. Such powers continued in various guises with the *Regulation of Investigatory Powers Act 2000*, and then the *Investigatory Powers Act 2016*.

---

<sup>34</sup> See ‘Of straws and haystacks’, Graham Smith (2018) Cyberleagle blog, available at: <https://www.cyberleagle.com/2014/11/of-straws-and-haystacks.html> and ‘Interception: law, media, and techniques’, Bernard Keenan (2017) The London School of Economics and Political Science, available at: <http://etheses.lse.ac.uk/3640/>.

<sup>35</sup> See §4 Official Secrets Act 1920 “Where it appears to a Secretary of State that such a course is expedient in the public interest, he may, by warrant under his hand, require any person who owns or controls any telegraphic cable or wire, or any apparatus for wireless telegraphy, used for the sending or receipt of telegrams to or from any place out of the United Kingdom, to produce to him, or to any person named in the warrant, the originals and transcripts, either of all telegrams, or of telegrams of any specified class or description, or of telegrams sent from or addressed to any specified person or place, sent or received to or from any place out of the United Kingdom by means of any such cable, wire, or apparatus, and all other papers relating to any such telegram as aforesaid”. Available at: <https://www.legislation.gov.uk/ukpga/Geo5/10-11/75/section/4/enacted/data.pdf>.

<sup>36</sup> The D-notice system is an arrangement between the government and media to ensure that journalists do not endanger national security. The D-notice affair, as it became known, occurred in 1967 when then U.K. Prime Minister Harold Wilson accused the defense correspondent of the Daily Express, Chapman Pincher, of ignoring D-notices by revealing that the secret services were scrutinizing thousands of private cables and telegrams sent from Britain without obtaining the necessary Official Secrets Act warrant. The Radcliffe Report is the Report of the Committee of Privy Counsellors Appointed to Inquire into “D” Notice Matters. See p.125 ‘Interception: law, media, and techniques,’ Bernard Keenan (2017), The London School of Economics and Political Science, available at: <http://etheses.lse.ac.uk/3640/>.

### Official Confirmation

There was not a precise moment when the U.K. government officially confirmed the modern day practice of bulk interception. Instead, a slow elucidation of the matter in a variety of fora produced today's situation where there is a reasonably comprehensive, officially-sanctioned picture of the U.K.'s bulk interception practice.

The government's position is that to some degree, bulk interception was avowed with the passing of Section 8(4) of the *Regulation of Investigatory Powers Act 2000 (RIPA)*. Indeed, in the course of litigation the U.K. government has asserted "[t]he Government intercepts communications in "bulk" – including at the level of communications cables -- pursuant to the lawful authority of warrants under Section 8(4) RIPA."<sup>37</sup> However the then Independent Reviewer of Terrorism Legislation David Anderson QC has thrown his weight behind those who said that RIPA wasn't as clear on this point as it could have been and described the law as "obscure since its inception, [and] incomprehensible to all but a tiny band of initiates."<sup>38</sup>

It was with the publication of a report by the U.K. parliamentary oversight committee, the Intelligence and Security Committee, in 2013 that the position was clearly asserted in plain language that U.K. intelligence agencies use "bulk interception techniques [to] access internet communications on a large scale."<sup>39</sup> The report also set out some of the key technical issues for the first time, including how bearers are selected, alongside information about filtering processes and the selection of communications.

Further information about the legal position and technical practice were slowly provided during the course of disclosure in response to ongoing legal challenges primarily instigated by the NGO Privacy International. With the passing of the *Investigatory Powers Act 2016* "bulk interception warrants"<sup>40</sup> were enacted into law in plain language.

Ten human rights organizations brought claims under the RIPA regime against GCHQ alleging that that bulk interception practices violated human rights. The Investigatory Powers Tribunal – a specialist tribunal set up to hear claims against the U.K. security and intelligence agencies – found that GCHQ had unlawfully surveilled two of them, Amnesty International and the South African Legal Resources Center.

---

<sup>37</sup>U.K. Observations, May 2019.

<sup>38</sup> 'A Question of Trust', David Anderson QC, Independent Reviewer of Terrorism Legislation, (2015) available at: <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf>.

<sup>39</sup> 'Privacy and Security: A modern and transparent legal framework', The Intelligence and Security Committee of Parliament (2013) available at: [https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312\\_ISC\\_P%2BS%2BRpt%28web%29.pdf](https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf).

<sup>40</sup> §Chapter 1, Investigatory Powers Act 2016.

The Tribunal found that GCHQ intercepted the organizations' communications, and accessed them or selected them for examination, but errors were made, resulting in communications being held for longer than they should have been, or selected for examination in breach of GCHQ's internal guidelines.<sup>41</sup> The diagram (Fig. 8) sets how the court applied its reasoning to the unlawful retention of Amnesty International's communications by GCHQ.

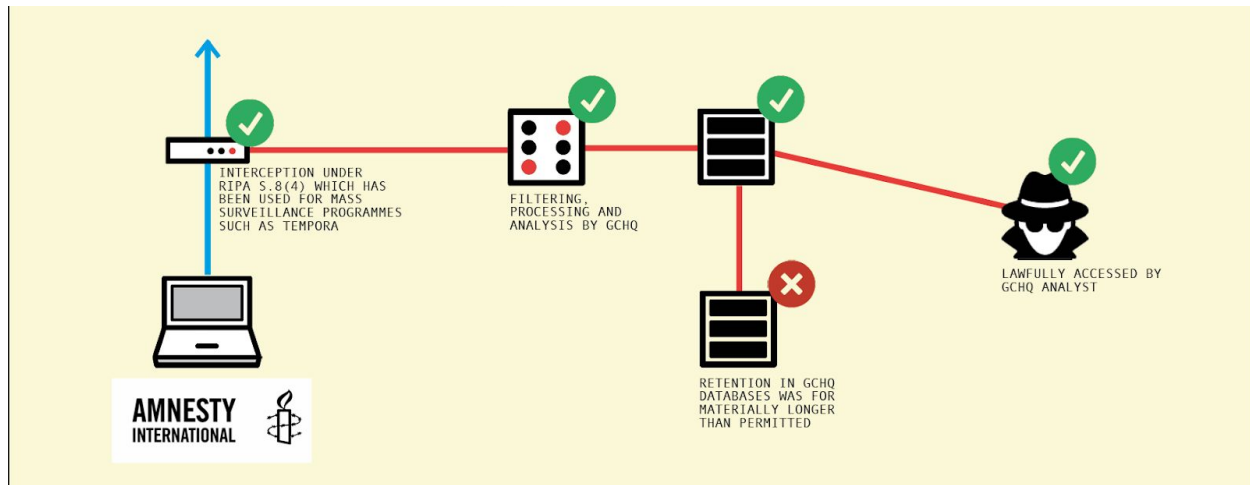


Fig. 8: [Diagram explaining the Tribunal's finding in Liberty & Others v U.K. IPT/13/77/H](https://www.ipt-uk.com/docs/Final_Liberty_Ors_Open_Determination_Amended.pdf)

The U.K. closely guards its national security and with respect to electronic surveillance, had been one of the most secretive among U.S. allies and intelligence partners. The fact that the U.K. government has been able to move from a position of neither confirming nor denying the practice of bulk cable interception to becoming one of the most transparent within a period of six years strongly suggests that a similar path could be taken by other countries without sacrificing national security.

#### Box - Big Brother Watch v U.K.

Following the Snowden revelations a number of civil liberties organizations filed legal complaints which were eventually considered by the European Court of Human Rights. The case referred to as Big Brother Watch and Others,<sup>42</sup> is actually three joined applications Big Brother Watch and Others v. the United Kingdom (no. 58170/13); Bureau of Investigative Journalism and Alice Ross v. the United Kingdom (no. 62322/14); and 10 Human Rights Organisations and Others v. the United Kingdom (no. 24960/15). The case deals with a number of issues relating to the U.K. surveillance regime, but principally the lawfulness, necessity, and proportionality of 1) bulk interception and 2) intelligence sharing between the NSA and GCHQ.

<sup>41</sup> Liberty & Others vs. the Security Service, SIS, GCHQ IPT/13/77/H (2015) available at: [https://www.ipt-uk.com/docs/Final\\_Liberty\\_Ors\\_Open\\_Determination\\_Amended.pdf](https://www.ipt-uk.com/docs/Final_Liberty_Ors_Open_Determination_Amended.pdf).

<sup>42</sup> Case of Big Brother Watch and Others v. the United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15), available at: <http://hudoc.echr.coe.int/eng?i=001-186048>.

The joined cases were heard by the Chamber, which found that 1) the U.K. bulk interception regime violated Convention rights to privacy and free expression (including highlighting there was insufficient oversight of the selection of internet bearers for interception, and safeguards around filtering, and selection for examination); and 2) the regime for sharing intelligence between GCHQ and NSA did not violate the European Convention on Human Rights.

The claimants appealed the decision from the Chamber, to the Grand Chamber, which agreed to review the case and deliver final judgment.

The U.K. government's "observations" cited in this report are the equivalent of a legal brief filed in a U.S. appellate court. CDT filed an intervention (equivalent to a brief amicus curiae in the U.S. system) in the case when it was being considered by the Chamber,<sup>43</sup> and its appeal to the Grand Chamber.<sup>44</sup>

### Legal Regime

The *Investigatory Powers Act 2016* sets out the conditions under which a bulk interception warrant may be sought and the purposes for which a warrant can be issued.<sup>45</sup>

Bulk interception warrants must be necessary for a statutory purpose in the interests of national security<sup>46</sup> or for the purpose of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security.<sup>47</sup>

The main purpose of the warrant must also be acquiring “overseas-related communications.” Notably this does not need to be the sole purpose, just the main purpose, and indeed internal U.K. communications are inevitably collected. Bulk interception warrants must also specify the operational purposes for which any intercepted communications obtained under the warrant may be selected for examination.

The inclusion of operational purposes is a new requirement introduced with the passage of the *Investigatory Powers Act 2016*. The list of operational purposes is not public, but an example of an

---

<sup>43</sup> “CDT & PEN American Center Intervene in Big Brother Watch vs. U.K. Case” (2016) available at: <https://cdt.org/insight/cdt-pen-american-center-intervene-in-big-brother-watch-vs-uk-case/>.

<sup>44</sup> “CDT Brief in Big Brother Watch and Others v. The United Kingdom,” (2019), available at: <https://cdt.org/insight/cdt-brief-in-big-brother-watch-and-others-v-the-united-kingdom/>.

<sup>45</sup> As well as the Investigatory Powers Act 2016, further information is provided in the Interception of Communications Code of Practice, as well as Advisory Notice 1/2018 Approval of Warrants, Authorisations and Notices by Judicial Commissioners published by the Investigatory Powers Commissions Office.

<sup>46</sup> §138(1)(b)(ii) Investigatory Powers Act 2016.

<sup>47</sup> §138(2) Investigatory Powers Act 2016.

operational purpose might be “attack planning by ISIL in Syria against the U.K.”<sup>48</sup> While illustrative, it might not be the case that operational purposes are in fact this detailed, as the Act itself only requires an operational purpose to be specified in a greater level of detail than the statutory purposes.<sup>49</sup> Additionally, the Act requires that the heads of the intelligence services must maintain a central list of all of the operational purposes, which have to be approved by the Secretary of State, reviewed by the Prime Minister, and shared every three months with the Intelligence and Security Committee of the U.K. Parliament.

The Interception of Communications Code of Practice<sup>50</sup> further sets out what is expected on the face of a bulk interception warrant. It must include a description of the communications to be intercepted, the details of any telecommunications operator(s) who may be required to provide assistance, and, where relevant, an assessment of the feasibility of the operation, which assessment of is normally based on information provided by the telecommunications operator.<sup>51</sup>

It is not known how many bulk interception warrants are in place under the *Investigatory Powers Act 2016*, but the government disclosed that interception under the previous legal regime (s.8(4) RIPA) took place under the authority of fewer than 20 warrants at any one time.<sup>52</sup>

While bulk interception warrants are submitted by the heads of the intelligence agencies, and when issued, are addressed to the person who submitted the application, the warrant will usually be served on a telecommunications operator to provide assistance in giving effect to it.<sup>53</sup> Bulk interception warrants have extraterritorial effect and can be served on overseas operators.<sup>54</sup>

Telecommunications companies can also be served with a technical capability notice<sup>55</sup> that requires them to provide and maintain a continuous capability to carry out interception under warrant. The government does not disclose the names of companies who have been subject to a technical capability notice, and the companies who receive a notice are under a duty not to disclose the existence or contents of that notice to any person, without the permission of the Secretary of State.<sup>56</sup> A company

---

<sup>48</sup> “Factsheet - Bulk Interception,” U.K. Government (2015) available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/473751/Factsheet-Bulk\\_Interception.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk_Interception.pdf).

<sup>49</sup> Namely, the interests of national security or the purpose of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security.

<sup>50</sup> The Interception of Communications Code of Practice is a statutory instrument which are used to provide practical measures that enable the law to be enforced and operate in daily life. Codes are legally binding and take primacy over any internal advice or guidance.

<sup>51</sup> §6.20(b) Interception of Communications Code of Practice.

<sup>52</sup> See “Interception under the s.8(4) Regime has taken place under the authority of fewer than 20 s.8(4) warrants at any one time,” U.K. Observations, May 2019.

<sup>53</sup> §6.7 Interception of Communications Code of Practice.

<sup>54</sup> §139 Investigatory Powers Act.

<sup>55</sup> §253 Investigatory Powers Act.

<sup>56</sup> §8.24 Interception of Communications Code of Practice.

subject to a notice must notify the Secretary of State if it proposes to change or upgrade its network in a manner that might jeopardize its ability to give effect to an ongoing notice.<sup>57</sup>

### *Bulk Collection in Practice*

The U.K. now has officially confirmed and provided both technical and legal detail about each key step of the cable interception process. The U.K. model is structured and tied to how the legal framework has developed over decades. It's discussed most recently by the U.K. government as a four step process:<sup>58</sup>

1. **Collection** - the process of selecting bearers to access [CCM - 1][CCM - 2.a.]
2. **Filtering** - the deployment of negative filters to discard unwanted traffic [CCM - 2.b.i]
3. **So called 'selection for examination'** - the automatic application of positive filters via simple and complex selectors to identify communications to retain [CCM - 2.b.ii]
4. **Examination** - human examination by an analyst [CCM - 4]

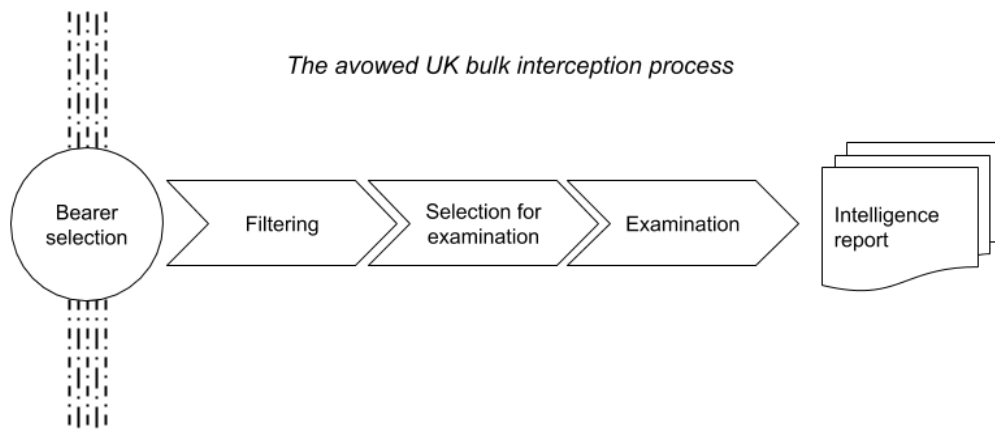


Fig. 9: Diagram created by report author Erik Kind for the purposes of this document.

### *Collection*

GCHQ will have probes [CCM - 2.a.ii] at significant cable landing points as well as other key infrastructure points. These probes provide the capacity to access the bearers when needed.

The U.K. government does not collect the communications from all bearers to which it has access [CCM - 2.a.ii]. While the U.K. government has said that approximately 100,000 bearers make up the global internet, the percentage that physically traverse or land in the U.K. is considerably smaller and the exact

<sup>57</sup> §8.35 Interception of Communications Code of Practice.

<sup>58</sup> The majority of government documents, and independent reports actually set out a three stage process, but in seeking to defend themselves before the Strasbourg court, the U.K. government has unpacked the last step which was 'selection for examination' into two steps called 'so called 'selection for examination'' and 'examination. See §31 U.K. Observations, May 2019.

number is not known. Likewise, the precise number of bearers on which GCHQ's systems operate is not officially confirmed, although the Intelligence and Security Committee has reported that GCHQ chooses "... only a small proportion of those that GCHQ are theoretically able to access"<sup>59</sup> and that "GCHQ's bulk interception systems operate on a small proportion of the bearers that make up the global internet."<sup>60</sup>

David Anderson's Bulk Powers Review confirmed "GCHQ does not have the capacity, or legal authority, to access every bearer in the world." But there is insufficient official information published to assess whether it is legal or technical issues that are placing the true limit on the number of bearers GCHQ's bulk interception systems operate on.<sup>61</sup>

To determine which bearers to prioritize and collect from, GCHQ uses a number of methods. There is an obligation in the Interception Code of Practice<sup>62</sup> that agencies must use their knowledge of how international communications are routed to intercept only from the most relevant bearers. In addition, surveys are also undertaken of the cables to assess the proportion of relevant material that is traversing them. In legal papers filed with the European Court of Human Rights, the U.K. government indicated that GCHQ will only select bearers that are carrying external communications of intelligence value. It said that to achieve this result, GCHQ will undertake "regular surveys of the contents of bearers: for example, a particular cable might carry a high proportion of communications to or from Syria."<sup>63</sup>

GCHQ staff have given on-the-record interviews confirming that they now are deploying machine learning to try and identify which bearers to select.<sup>64</sup>

---

<sup>59</sup> 'Privacy and Security: A modern and transparent legal framework', The Intelligence and Security Committee of Parliament (2013) available at: [https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312\\_ISC\\_P%2BS%2BRpt%28web%29.pdf](https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf).

<sup>60</sup> Factsheet - Bulk Interception (2015) Investigatory Powers Bill, available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/473751/Factsheet-Bulk-Interception.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk-Interception.pdf).

<sup>61</sup> §2.15 Bulk Powers Review, David Anderson (2016), available at: <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf>.

<sup>62</sup> "6.10 When conducting bulk interception, an intercepting authority must use its knowledge of the way in which international communications are routed, combined with regular surveys of relevant communications links, to identify those individual communications links that are most likely to contain overseas-related communications, which will be relevant to the operational purposes specified on a warrant." Interception Code of Practice

<sup>63</sup> 'Observations of the Government of the United Kingdom on the Admissibility and Merits of the Application', Big Brother Watch v U.K. Application No. 58170/13, (Sept 2017) available at: <https://privacyinternational.org/sites/default/files/2018-02/BBW%26Ors%2C10HROrgs%2CBIJ%26Anr%20-%20Gov%20Observations%20-%202-10-17.pdf> [hereinafter referred to as U.K. Observations on Admissibility and Merits, Sept 2017].

<sup>64</sup> "I am back behind the barbed-wire fences at Cheltenham to meet Paul, a senior director who leads a team looking at how GCHQ develops its next-generation artificial intelligence capabilities. He and his colleague Steve have created a new program that uses machine learning to identify the best internet access points for collecting data. It is based on the open-source algorithms developed by Google's artificial intelligence arm DeepMind to teach a computer how to win at chess. If successful, it could transform the way GCHQ gathers internet data. [...] Paul explains: "What the machine can learn is that there are patterns that are better than me just plugging into the



Once bearers are selected or accessed, then a copy of everything flowing through it is collected including communications and associated communications data.<sup>65</sup>

### Filtering

Once selected, the copy of the bearer then enters a multi-stage processing environment. The initial stage is filtering [CCM - 2.b]. The purpose of this is to “automatically discard in near-real time a significant proportion of the communications and communications data on the targeted bearers, on the basis that it comprises the traffic of a type least likely to be of intelligence value.”<sup>66</sup> The Interception Code of Practice describes this step as providing a “degree of filtering”<sup>67</sup> that “will vary between processing systems.”<sup>68</sup>

This step is perhaps best understood as a negative filter [CCM - 2.b.i], which is seeking to identify material to discard. It is imagined that this is likely to be material from streaming services like Netflix or Spotify which are high bandwidth and a non-trivial percentage of the global internet flows, but which usually contain little of intelligence value.

*Filtering Internal U.K. Communications: A significant point of discussion in Europe has been whether an intelligence agency is able to successfully filter out domestic communications when undertaking foreign-focused cable interception. The U.K. Interception Code of Practice explains that “[d]ue to the global nature of the internet, the route a particular communication will take is hugely unpredictable. This means that a bulk interception warrant may intercept communications between individuals in the British Islands.” There are a number of issues that flow from this as to the legality and proportionality of the bulk interception powers, but this report will not delve into them.*

### Selection for Examination

The remaining communications are then passed through a positive filter [CCM - 2.b.ii], to further process the communications that are responsive to a variety of different selectors, before they are looked at by a human analyst. This stage is an automated process, sifting the intercepted material, and extracting any communications that match selection criteria.

The selection criteria may be simple or complex. Simple criteria using “strong selectors” are items such as telephone numbers or email addresses. Complex criteria use “complex queries” that combine a

---

*internet and hoping. From the computer’s perspective, it’s playing and it knows what good looks like. It knows intelligence reports are being generated [from the data collected] and it is trying to create different rules and guess better than a human would ever do.” GCHQ says the project, which has been running for six months, requires much more testing before it can be rolled out.” ‘Inside GCHQ: the art of spying in the digital age’ David Bond (2019) Financial Times, available at: <https://www.ft.com/content/ccc68ffc-7c1e-11e9-81d2-f785092ab560>.*

<sup>65</sup> “In practical terms, ‘accessing’ means making a copy of the communications and associated communications data flowing down the bearer.” U.K. Observations, May 2019.

<sup>66</sup> U.K. Observations, May 2019.

<sup>67</sup> §6.6 Interception Code of Practice.

<sup>68</sup> §6.6 Interception Code of Practice.



number of criteria “which may include weaker selectors but which in combination aim to reduce the odds of a false positive.”<sup>69</sup>

Examples of “strong selectors” that have been avowed by the U.K. government are limited to telephone numbers or email addresses.<sup>70</sup> More detailed examples have been provided of “complex queries” which are “used where GCHQ is looking to match much more complicated criteria, for example with three or four elements.”<sup>71</sup>

Examples of complex queries using (presumably weaker selectors) provided by the U.K. government include “searching for material which combined use of a particular language, emanation from a particular geographical region, and use of a specific technology” or “a complex digital signature created by a particular machine used in cyber attacks, or the use of a call sign from a particular vessel”<sup>72</sup> or a “complex query” designed to identify individuals “accessing known extremist literature, where that was combined (say) with being in a particular location such as northern Iraq; or using a particular software application associated with terrorism.”<sup>73</sup>

Communications that match the selectors are retained for possible future processing, or for future examination by an analyst. As the government explains “[t]his stage does not entail the production of any intelligence; it merely sifts the material which an analyst may be authorized to view.”<sup>74</sup>

This aspect, and particularly how the technical step matches the legal framework, had been unclear. However, in recent documents, the U.K. government has explained that “[t]he phrase “selection for examination” is capable of misleading”<sup>75</sup> but that “[a]s used by the Intelligence Services, it refers to the *automated* process of conducting simple or complex searches of intercepted material, in order to create a list of communications from which an analyst may potentially choose items to inspect.”<sup>76</sup>

There isn’t a separate legal process on the face of the statute or in the codes of practice that spells out how selectors are chosen and deployed on the processing systems. However, the government has stated that “[w]hen a new selector is added to the system, the analyst adding it needs to complete a written record, explaining why it is necessary and proportionate to apply the selector for purposes within the Secretary of State’s certificate. In the case of a ‘strong selector,’ the analyst would need to

---

<sup>69</sup> §15 ‘Further Observations of the Government of the United Kingdom’, *Big Brother Watch v U.K.* Application No. 58170/13, (Dec 2016) available at: <https://privacyinternational.org/sites/default/files/2018-02/2016.12.16%20Government%27s%20further%20obs.pdf> [hereinafter referred to as U.K. Further Observations, Dec 2016].

<sup>70</sup> Leaked documents provide a much wider list of ways in which GCHQ selects communications.

<sup>71</sup> §2.19(b) Bulk Powers Review, David Anderson (2016), available at: <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf>.

<sup>72</sup> §35 U.K. Observations, May 2019.

<sup>73</sup> §47 U.K. Observations, May 2019.

<sup>74</sup> §31(3) U.K. Observations, May 2019.

<sup>75</sup> §9(3) U.K. Observations, May 2019.

<sup>76</sup> §9(3) U.K. Observations, May 2019.

explain (for example) the justification for seeking the communications of a particular target; how the selector related to the target's methods of communicating; and why selection of the relevant communications would not involve an unacceptable degree of collateral intrusion into privacy."<sup>77</sup>

While there is no published guidance underpinning how checks take place, the U.K. government has said that "[s]electors applied directly to bearers are subject to a rigorous process of automated rules, augmented by human intervention where necessary, to ensure that they meet the appropriate legal and policy requirements."<sup>78</sup>

A similar process is in place for the deployment of "complex queries" where an analyst would "need to develop selection criteria most likely to identify communications bearing intelligence of value; and would similarly need to explain why the criteria were justified, and why their use would be necessary and proportionate for purposes within the Secretary of State's certificate."

Depending on how this automatic "selection for examination" is deployed, communications can be buffered within them for different periods of time. Oversight reports confirmed that "[a] copy of all the communications on a bearer has to be held for a short period in order to allow the strong selectors to be applied to those communications, although the government has also stated that the simple "strong selector" process essentially works in "near real time." However, the "complex query" process, takes longer, and in recent statements to the court, it's suggested that this period is a "few days."<sup>79</sup>

It is not known for how long selectors are permitted to be deployed on GCHQ bulk processing systems. However, if they are used for target development or target discovery, they may remain in use for a maximum of three months before they are reviewed.<sup>80</sup>

Communications that are selected for examination via this automated process are by default retained for "no longer than a few months."<sup>81</sup> If material is used in an intelligence report, the report will be retained.

There are officials who may also be permitted to access the system during the processes of filtering, processing and selection for examination, for example to check system health,<sup>82</sup> or to "to check whether the selection methodology remains up-to-date and effective."<sup>83</sup> Selectors must be stored in an approved location, and they are audited by the U.K. independent oversight body, the Investigatory Powers Commissioners Office.<sup>84</sup>

---

<sup>77</sup> §35 U.K. Observations, May 2019.

<sup>78</sup> §35 U.K. Observations, May 2019.

<sup>79</sup> §63 U.K. Observations, May 2019.

<sup>80</sup> §36 U.K. Observations, May 2019.

<sup>81</sup> §40 U.K. Observations, May 2019.

<sup>82</sup> §6.72 Interception Code of Practice.

<sup>83</sup> §34 U.K. Observations, May 2019.

<sup>84</sup> "Any selector must be as specific as possible, in order to select the minimum material necessary for the intelligence purpose, and to be proportionate. If, through analysis, it is established that selectors are not being used

## Examination

Communications are then provided to analysts who are able to examine them [CCM - 3].

Not all communications that are “selected for examination” are examined by a human analyst. The government states that “[o]nly a fraction of those communications selected for possible examination by either of the processing systems set out above is ever in fact looked at by an analyst.”<sup>85</sup>

If communications were selected via the “strong selector” process, the U.K. government has explained that a further automated triage process is in place. This assists in helping analysts further sift irrelevant material, but also prioritize which communications are important for specific targets.<sup>86</sup>

If communications were selected according to the “complex query” process, “items are presented to analysts as a series of indexes in tabular form showing the result of searches.”<sup>87</sup> The government has proposed that this should be imagined as similar to reviewing the results of a search engine.<sup>88</sup>

Before an analyst can examine material, they need to provide a record setting out why the material is required, and how examining it is lawful and proportionate. GCHQ systems prevent access to material unless a record is created.<sup>89</sup>

## Conclusion

In a relatively short time frame, the U.K. has transformed its legal framework governing bulk interception, and in doing so, has published detailed information, ensured there was public debate and independent reviews, and all without damaging national security. That such a feat was possible, particularly from such a close intelligence partner, should be a clear indication that the U.S. is able to go considerably further in its transparency efforts without posing a grave threat to national security.

---

*by their intended target, prompt action must be taken to remove them from relevant systems. The use of selectors must be recorded in an approved location that enables them to be audited; creates a searchable record of selectors in use; and enables oversight by the Commissioner,” §35 U.K. Observations, May 2019.*

<sup>85</sup> §33(1) U.K. Observations on Admissibility and Merits, Sept 2017.

<sup>86</sup> §35(1) U.K. Observations on Admissibility and Merits, Sept 2017.

<sup>87</sup> §35(2) U.K. Observations on Admissibility and Merits, Sept 2017.

<sup>88</sup> “In simple terms, this can be considered as an exercise similar to that conducted when deciding what search results to examine, from a list compiled by a search engine such as Bing or Google. The remainder of the potentially relevant items are never opened or read by analysts”, §33(2) U.K. Observations on Admissibility and Merits, Sept. 2017.

<sup>89</sup> §3 U.K. Observations, May 2019.

## Sweden

Sweden led the world in officially debating bulk interception of fiber optic cables crossing the Swedish border as early as 2006.<sup>90</sup> The law governing bulk cable collection passed in 2008, and Sweden has shared oversight reports publicly covering filtering and selection since 2010. They remain one of the most transparent countries when it comes to describing law and practice.

The *Signals Intelligence Act 2008* permits the bulk collection in pursuit of eight enumerated purposes.<sup>91</sup> This is done by obliging telecommunications companies to route traffic to a “hand-over point.” The telecommunications company is not involved in any filtering of the communication or data.<sup>92</sup> Instead the Foreign Intelligence Inspectorate, an independent control and oversight body, which controls the “hand-over point” provides access to specific cables to the FRA according to the permit requirements that are in place.<sup>93</sup> The Foreign Intelligence Inspectorate acts as a privacy safeguard and gatekeeper to the cable network, permitting or denying access by the FRA.

The Swedish Government has set out a six-stage signals intelligence or bulk collection process:<sup>94</sup>

- 1) Signal identification and extraction, within the bounds of Swedish law and with “regard to the practical limitations of the FRA’s collection, processing, and analysis capacity”. [CCM - 2.a]
- 2) “[A]utomatic collection selectors are applied [...] “in order to intercept and gradually reduce what is finally collected.” This has two stages. First, “data reduction at signals level is carried out, which means that only certain signals are chosen for further processing.” Second, “data reduction is carried out at communications level, which means that selectors are applied to the

<sup>90</sup> “[T]he Government would like to point to the fact that signals intelligence conducted on fiber-optic cables may only concern communications crossing the Swedish border in cables owned by a network operator,” ‘Observations of the Government of Sweden’, Centrum för rättvisa v. Sweden Application no. 35252/08, available at: [http://centrumforrattvisa.se/wp-content/uploads/2019/07/35252-08file35252\\_08\\_GVT\\_further\\_OBS\\_ENG\\_GC\\_.pdf](http://centrumforrattvisa.se/wp-content/uploads/2019/07/35252-08file35252_08_GVT_further_OBS_ENG_GC_.pdf) [hereinafter referred to as Sweden Observations, May 2019].

<sup>91</sup> “The purposes for which electronic signals may be collected as part of foreign intelligence are specified in the Signals Intelligence Act which provides that signals intelligence may be conducted only to survey 1) external military threats to the country, 2) conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations, 3) strategic circumstances concerning international terrorism or other serious cross-border crimes that may threaten essential national interests, 4) the development and proliferation of weapons of mass destruction, military equipment and other similar specified products, 5) serious external threats to society’s infrastructure, 6) foreign conflicts with consequences for international security, 7) foreign intelligence operations against Swedish interests, and 8) the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy” § 1(2)) Signals Intelligence Act (2008:717).

<sup>92</sup> ‘FRA and the European Convention on Human Rights - A Paradigm Shift in Swedish Electronic Surveillance Law’, Mark Klamberg (2016).

<sup>93</sup> Chapter 6, section 19a of the Electronic Communications Act (Lagen om elektronisk kommunikation; 2003:389).

<sup>94</sup> §3.4.44 ‘Appendix 1 to the Observations of the Government of Sweden’, Centrum för rättvisa v. Sweden Application no. 35252/08, available at: <https://cdt.org/files/2019/09/35252-08-file-35225-08-Annex-1-3-to-GVT-further-OBS.pdf> [hereinafter referred to as Appendix to Sweden Observations, May 2019].

remaining information to sift out communications that are relevant to foreign intelligence,”<sup>95</sup>  
This phase “is done in real time or near real time”.<sup>96</sup> [CCM - 2.b]

- 3) Further processing to “refine the information and make it as easily usable as possible from an analysis perspective” such as data structuring and language translation.
- 4) Analysis “merging fragments of information to a greater picture, drawing conclusions, establishing facts as well as hypothesis”. [CCM - 3]
- 5) Report dissemination to intelligence customers. [CCM - 4]
- 6) “[F]eedback on use and effect of the intelligence provided.”

Under the *Signals Intelligence Act 2008*, warrants have to specify the “signal carriers,” the selectors or categories of selectors, and other conditions to limit the interference with personal integrity.<sup>97</sup> There are reasonably detailed descriptions of the types of queries and selectors used.<sup>98</sup> Sweden does not publish information about how many “signal intelligence permits” or warrants are in place,<sup>99</sup> but these permits have a maximum six-month duration. Selectors are not automatically removed, and the government has confirmed that some approved selections may remain in place for several years.<sup>100</sup>

Parliamentary oversight committees in Sweden, such as the Signals Intelligence Committee, have monitored and reported publicly on how signals intelligence collection is undertaken by the FRA.<sup>101</sup> Their reports include a discussion of the difficulty in separating domestic cable-based communications from those crossing the Swedish border, and the steps the FRA takes to mitigate that, such as separating

---

<sup>95</sup> §4.1.3.62 Appendix to Sweden Observations, May 2019.

<sup>96</sup> §4.1.3.63 Appendix to Sweden Observations, May 2019.

<sup>97</sup> §4.2.75 Appendix to Sweden Observations, May 2019.

<sup>98</sup> “Selectors refer to a combination of technical data and various addressing details. The more detailed formulation of selectors is achieved through a carefully balanced combination of technical data, such as the source country of the signals gathered and the transmission media with which they are communicated, as well as other parameters such as keywords (e.g. the specific name of a weapons system or other technical terminology), unique names and languages. The various components also include frequencies, telephone numbers or IP addresses. Names, telephone numbers and email addresses, and IP addresses that can be linked to a specific individual, may only be used if it is of particular importance for the activities. The selectors are built up with great precision, which means that they consist of several components. By specifying selectors, the FRA can search through a signal and find the items in which the selector appears. All parts must match to get a hit in the traffic collected. The selectors are intended to make searches accurate and to serve as a kind of filter to limit intelligence collection to what is relevant, as well as to prevent unlawful intelligence collection.” Sweden Observations, May 2019.

<sup>99</sup> “The Government wishes to state that this kind of information could be indicative of the ability and methods of the FRA in a manner incompatible with the purposes of signals intelligence. It is therefore not possible to inform the Court about the annual number of permits.” Sweden Observations, May 2019.

<sup>100</sup> “Foreign intelligence is a long-term activity which means that the need for using certain approved selectors in a signals intelligence mission may need to extend for several years. This can be clearly illustrated, inter alia, by the requirement to map foreign military activity around the borders of Sweden.” Sweden Observations, May 2019.

<sup>101</sup> The Signals Intelligence Committee was a temporary expert committee appointed by the Government to follow up the implementation of the Signals Intelligence Act and related legislation in 2011. It is not a permanent parliamentary oversight committee. Indeed, no permanent parliamentary oversight committee is specifically tasked with overseeing the activities of the FRA.

communications manually at the processing or analyzing stage.<sup>102</sup> The Swedish Signals Intelligence Committee also undertook reviews to ensure the FRA's use of selectors is compatible with the permits that have been issued. This included analysis of selectors used for the collection of data about the conditions for Sweden's participation in peace support and humanitarian operations.<sup>103</sup>

The Foreign Intelligence Inspectorate, an oversight body with a board constituted of former or current judges and parliamentarians,<sup>104</sup> has also undertaken a number of audits of the use of selectors. Between 2010 and 2014, the Inspectorate audited the FRA's use of selectors on 17 occasions, issuing recommendations for change after one audit. In the period from 2015 to 2018, the Inspectorate audited the FRA's use of selectors on 11 occasions with no recommendations made.<sup>105</sup>

The Swedish government has acknowledged that the FRA could, in theory, collect all communications from all cables to which it has access, however the government has stated that such an act would "constitute a disproportionate interference in the personal privacy [and] [t]his approach would also require unrealistic capacity for the storage of data that would only be of very limited relevance to signals intelligence."<sup>106</sup>

The seven "data compilations" that can be held at the FRA are enumerated in law, such as for "raw material" or for "information on the signals environment" along with set retention periods for each "data compilation."<sup>107</sup> Any unprocessed or automatically processed data collected must be discarded no later than one year after the processing of the data began, as per the *FRA Personal Data Processing Ordinance*.<sup>108</sup>

Bulk communications data intercepted from cables are also "used to establish a picture of normal communications patterns for reference when detecting anomalies."<sup>109</sup> Any internal Swedish to Swedish

<sup>102</sup> Centrum för rättvisa v. Sweden (Application no 35252/08), available at: <http://hudoc.echr.coe.int/eng?i=001-183863>.

<sup>103</sup> Unofficial translation of the Swedish Foreign Intelligence Inspectorate's Annual Report 2018; as provided in Centrum för rättvisa v. Sweden, 14.(1) [GOVT] Annex 13 <https://cdt.org/files/2019/09/14-I-GOVT-Annex-13.pdf>.

<sup>104</sup> See "The Foreign Intelligence Inspectorate is led by a board whose members are appointed by the Government on terms of at least four years. The president and the vice-president shall be or have been permanent judges. Other members are selected from candidates proposed by the party groups in the Parliament" §4.6.1.123 Appendix to Sweden Observations, May 2019.

<sup>105</sup> §4.6.1.1.133 Appendix to Sweden Observations, May 2019.

<sup>106</sup> §4.1.5.69 Appendix to Sweden Observations, May 2019.

<sup>107</sup> §4.4.1.90 Appendix to Sweden Observations, May 2019.

<sup>108</sup> "Finally, the FRA Personal Data Processing Act and its associated ordinance contain rules about discarding personal data. According to the main rule, personal data that is processed automatically must be discarded as soon as the data is no longer needed for the purposes for which it was processed. This is equivalent to the EU regulation on the processing of personal data. In any circumstances, unprocessed and automatically processed data collected in foreign intelligence and development activities must be discarded no later than one year after the processing of the data began, i.e. when it was collected (see the FRA Personal Data Processing Ordinance as described in Appendix 1, Section 4.4)". Sweden Observations, May 2019. The FRA Personal Data Processing Ordinance, is a Government Ordinance and not primary legislation.

<sup>109</sup> Sweden Observations, May 2019.

communications that are incidentally collected when undertaking bulk interception are required to be destroyed as soon as they are identified.<sup>110</sup>

Similarly to other European countries, network operators are required to perform their task facilitating interception such that the activities are not disclosed to third parties.<sup>111</sup>



## Germany



Germany has similar levels of transparency as the U.K. and Sweden, with statutes clearly regulating bulk cable interception activity, but perhaps leads the world in the public discussion of the technical details underpinning the practice thanks to work by its Parliamentary Committee of Inquiry.

Bulk cable interception by the German Federal Intelligence Service (BND) is avowed in Germany, with two statutes expressly regulating the practice.<sup>112</sup> The *BND Act* permits broad monitoring of international telecommunications to identify or counter “threats to the Federal Republic of Germany’s internal or external security”<sup>113</sup> and the *G10 Act* authorizes the BND to monitor international telecommunications to identify or counter specific threats.<sup>114</sup>

The *BND Act* governs foreign interception unless the communication involves at least one participant who is either a German national or a foreigner staying in Germany at which point it is instead regulated by the *G10 Act*.<sup>115</sup>

The regulation of foreign-to-foreign interception is a recent development that was introduced in December 2016 as part of *BND Act* reforms. Other reforms included expanding definitions so the BND can use technical equipment to collect personal data from ‘telecommunications nets’ which has a

---

<sup>110</sup> “[I]f communications have been intercepted between a sender and receiver both in Sweden, they must be destroyed as soon as their domestic nature has become evident.” Sweden Observations, May 2019.

<sup>111</sup> §4.1.3.61 Appendix to Sweden Observations, May 2019.

<sup>112</sup> ‘Germany’s intelligence reform: More surveillance, modest restraints and inefficient controls’, Thorsten Wetzling (2017) SNV, available at: [https://www.stiftung-nv.de/sites/default/files/snv\\_thorsten\\_wetzling\\_germanys\\_foreign\\_intelligence\\_reform.pdf](https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf).

<sup>113</sup> § 6(1)1 BND Act.

<sup>114</sup> These threats include: “Armed attack against Germany; international terrorist attack with a direct link to Germany; international proliferation of certain weapons, related goods, computer programs, and technologies; organized drug trafficking into the EU with a link to Germany; interference with the currency stability in the Euro-zone through counterfeiting; internationally organized money-laundering; organized smuggling of foreign nationals into the EU with a link to Germany; certain cyberattacks with a link to Germany” as per ‘Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden’ Christian Schaller, German Law Journal Vol. 19 No. 04, available at: [https://www.cambridge.org/core/services/aop-cambridge-core/content/view/494F82EE78DCF2709B07A2B57D95454C/S2071832200022926a.pdf/strategic\\_surveillance\\_and\\_extraterritorial\\_basic\\_rights\\_protection\\_german\\_intelligence\\_law\\_after\\_snowden.pdf](https://www.cambridge.org/core/services/aop-cambridge-core/content/view/494F82EE78DCF2709B07A2B57D95454C/S2071832200022926a.pdf/strategic_surveillance_and_extraterritorial_basic_rights_protection_german_intelligence_law_after_snowden.pdf).

<sup>115</sup> This is due to privacy guarantees offered by Article 10 of the German Basic Law.



definition broader than just telecommunications cables or networks, and includes collecting from infrastructure through which domestic German-to-German communications are transiting.<sup>116</sup>

The *BND Act* prohibits the BND from using search terms relating to a German national.<sup>117</sup> [CCM - 2.b] If data is collected about German nationals, domestic legal persons, domestic legal entities, or foreign nationals staying in Germany, the data, once identified as such, has to be deleted unless there is a separate authorization in place under the *G10 Act*. To segregate the communications that are entitled to these additional protections, the BND deploys technical filter rules known as the DAFIS filter system. [CCM - 2.b]

These technical filters work in three stages according to Electrospace.<sup>118</sup> Stage one is the application of a negative filter [CCM - 2.b.i] to remove any email addresses ending with .de or phone number starting with 0049. Stage two is a positive filter [CCM - 2.b.ii], which removes any communications that matches a list of roughly 30,000 identified known individuals such as foreign phone numbers or email addresses used by German citizens. Stage 3 seeks to filter out selectors that would conflict with German interests reportedly covering about 500 terms.<sup>119</sup> [CCM - 2.b.i]

These filters are not proactively developed, but instead are reactive and new terms are added once problems arise. For example, a foreign phone number would be added to the selector checklist at stage two when an analyst notices that a German is using it.

There was a significant scandal in Germany regarding the deployment of NSA selectors on BND systems, and the subsequent sharing of intercepted material back to NSA once collected. The NSA selectors were never publicly disclosed, despite multiple legal cases brought seeking to disclose them. The German parliament sued the German government for refusing to provide the NSA selectors to the Committee of Inquiry which was set up to investigate mass surveillance and the implications of the Snowden revelations.<sup>120</sup> The G10 Committee which approves and reviews actions taken under the *G10 Act* also sued the government to gain access to the NSA sectors but was also unsuccessful.

The *BND Act* doesn't require search terms to be expressly listed in authorization applications (which are made by the BND, prepared by the Chancellery, and presented to the Independent Committee of judicial

---

<sup>116</sup> § 6(1) BND Act.

<sup>117</sup> § 5(2)(lit. 1), (2)3. G10 Act.

<sup>118</sup> 'German BND didn't care much about foreign NSA selectors', Electrospace.net (2015) available at: <https://electrospace.blogspot.com/2015/05/german-bnd-didnt-care-much-about.html#dafis>.

<sup>119</sup> 'German BND didn't care much about foreign NSA selectors', Electrospace.net (2015) available at: <https://electrospace.blogspot.com/2015/05/german-bnd-didnt-care-much-about.html#dafis>.

<sup>120</sup> Constitutional Court, 2 BvE 2/15, Oct. 13, 2016, available at: [http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/10/es20161013\\_2bve000215.html](http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/10/es20161013_2bve000215.html).



review for approval)<sup>121</sup> unless search terms relate to EU institutions or authorities of EU Member States, which requires separate authorization.<sup>122</sup>

Authorization applications (made by the BND, prepared by the Chancellery, and presented to the G10 Commission for approval), under the *G10 Act* require expressly listing search terms.<sup>123</sup> The *G10 Act* also requires the identification of a geographic area of a certain state as the target. An order under the *G10 Act* also requires identifying the bearers (or “transmission channels”), and the percentage of those bearers which should be subjected to surveillance. [CCM - 2.a] There is a fixed limit of 20% of the capacity of ‘transmission channel’ that can be subjected to surveillance, however it is disputed how that should be calculated (e.g. available capacity, actual data transmitted, etc.).<sup>124</sup> The government claims that “on average, around 5 percent of traffic is accessed, the agreed upper limit of 20 percent of traffic is almost never exhausted.” This has been disputed by media reports.<sup>125</sup>

A large quantity of specific detail about international cable interception operations by the BND have been presented in public during the Committee of Inquiry. Evidence has been given by BND engineers who specialize in cable interception. They describe how probes are placed on cables, how they undertake their initial cable selection, how they cache data before selection, and even the quantity of selected metadata that is processed.<sup>126</sup>

The Committee of Inquiry ran from 2014 to 2017 and produced a 2,000-page report, currently only available in German.<sup>127</sup> A 300-page minority report was also published by dissenting members of the

---

<sup>121</sup> See “The reform created the Independent Committee (Unabhängiges Gremium - UG), a second German authorization body for strategic surveillance. Situated at the Federal Court of Justice in Karlsruhe, the UG provides ex ante authorization of strategic foreign-to-foreign communications data surveillance by the BND. It consists of three members plus three deputies. Its president and one member must be judges at the Federal Court of Justice. The third member must be a federal public prosecutor at that court” ‘Germany’s intelligence reform: More surveillance, modest restraints and inefficient controls’, Thorsten Wetzling (2017) SNV, available at: [https://www.stiftung-nv.de/sites/default/files/snv\\_thorsten\\_wetzling\\_germanys\\_foreign\\_intelligence\\_reform.pdf](https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf).

<sup>122</sup> See “The use of selectors that target public bodies of EU member states or EU institutions is restricted to 12 warranted cases and requires orders that mention the individual search terms (Section 9.2)” ‘Germany’s intelligence reform: More surveillance, modest restraints and inefficient controls’, Thorsten Wetzling (2017) SNV, available at:

[https://www.stiftung-nv.de/sites/default/files/snv\\_thorsten\\_wetzling\\_germanys\\_foreign\\_intelligence\\_reform.pdf](https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf).

<sup>123</sup> § 10(4) G10 Act.

<sup>124</sup> § 10(4) G10 Act.

<sup>125</sup> ‘Secret test report: How the BND thwarts the statutory 20 percent rule (updates)’, Andre Meister (2015)

Netzpolitik, available at:

<https://netzpolitik.org/2015/geheimer-pruefbericht-wie-der-bnd-die-gesetzlich-vorgeschriebene-20-prozent-regel-hintertreibt/>.

<sup>126</sup> ‘Live blog from the intelligence committee of inquiry’, Netzpolitik, (2014) available at:

<https://netzpolitik.org/2014/live-blog-aus-dem-geheimdienst-untersuchungsausschuss-bnd-mitarbeiter-k-l-und-p-auf-der-zeugebank/>.

<sup>127</sup> ‘Committee of Inquiry report into mass surveillance’, German parliament (2017)

<https://dipbt.bundestag.de/doc/btd/18/128/1812850.pdf>.

committee, which is also currently only available in German.<sup>128</sup> The summary of the dissenting report has been unofficially translated into English by one of the authors. This includes conclusions that “[b]etween 2005 and 2008, as part of the joint BND/NSA Operation Eikonal, the BND engaged in data tapping in Frankfurt am Main without legal authorization.”<sup>129</sup> The report also found that the DAFIS filter system shouldn’t have been used as it didn’t reliably filter out data protected by the G10 Act. The conclusion that the DAFIS filter system didn’t work was echoed by the German Data Protection Commissioner who said that the filter “has substantial systemic deficits.”<sup>130</sup> [CM - 2.b]



## The Netherlands

The Dutch Government has taken significant steps to inform the public about its bulk cable interception practices. It enacted legislation that gave its intelligence agencies new powers to intercept from fiber optic cables, and subjected those new powers to extensive independent review. The government has published a detailed chart showing how it collects, filters, stores, and uses information collected through bulk cable interception and even held an advisory referendum when considering the legislation.<sup>131</sup> A number of oversight reports are shortly due to be published which will further provide detail on key aspects of the bulk interception process.

The Dutch intelligence agencies were historically prohibited from undertaking bulk cable interception. With the passage of the *Intelligence and Security Services Act 2017 (Wiv 2017)*, the two Dutch intelligence agencies, the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD), have new powers to intercept from and select traffic from within fiber optic cables. [CCM - 2]<sup>132</sup> These new powers are modeled on existing bulk interception powers of satellite communication and radio traffic. Once intercepted, selectors are deployed against communications content [CCM - 2.b.ii]. Metadata is extracted in bulk and used for “automated data-analysis,” which includes developing profiles and pattern matching or to discover possible patterns.<sup>133</sup>

---

<sup>128</sup> Dissenting Committee of Inquiry report available semi-officially at:

[https://cdn.netzpolitik.org/wp-upload/2017/06/2017-06-20\\_NSAUA-Sondervotum-Opposition-geschwaerzt.pdf](https://cdn.netzpolitik.org/wp-upload/2017/06/2017-06-20_NSAUA-Sondervotum-Opposition-geschwaerzt.pdf).

<sup>129</sup> “*Weapons of Mass Surveillance – the German Snowden Inquiry*,” (2018) Anne Roth, available at:

<https://annalist.noblogs.org/post/2018/02/14/weapons-of-mass-surveillance-german-snowden-inquiry/>.

<sup>130</sup>

<https://netzpolitik.org/2016/secret-report-german-federal-intelligence-service-bnd-violates-laws-by-the-dozen/>.

<sup>131</sup> “Final results show majority of Dutch citizens votes against dragnet surveillance law,” Bits of Freedom (2018), available at:

<https://www.bitsoffreedom.nl/2018/03/22/intermediate-results-show-majority-of-dutch-citizens-votes-against-intelligence-law/>. Though a majority of the Dutch citizens opposed the legislation, it became law nonetheless because the referendum was not binding.

<sup>132</sup> §48-50 Wiv 2017.

<sup>133</sup> “*The Wiv 2017, A critical contemplation of the Act in an international context*,” Lotte Houwing, citing Art. 60 para. 2 Intelligence and Security Services Act 2017.

The Review Committee on the Intelligence and Security Services (CTIVD), an independent expert oversight body, has undertaken a number of reviews into the implementation of *Wiv 2017*.<sup>134</sup> Separate investigations into how the AIVD and MIVD were selecting traffic when intercepting fiber optic cables are also being undertaken. These investigations are into the application of 'filters' [CCM - 2.b] during bulk interception of communications, and the application of 'selection' during bulk interception of communications [2.b.ii].<sup>135</sup> In its progress report, the CTIVD concluded that there was "a high risk of irregularities where it concerns compliance with the target requirement and obligation to reduce data." Under the new investigation, the CTIVD is assessing whether the selection criteria are sufficiently targeted, the relevance of the selectors to the investigation, and whether irrelevant data is destroyed promptly.<sup>136</sup>

While, Ministers have stated that 98% of the intercepted data is expected to be deleted,<sup>137</sup> the use of these powers is still being challenged by a coalition of lawyers, journalists, technology companies, and civil society organizations, including the Dutch civil liberties organization Bits of Freedom.<sup>138</sup> The Dutch government has produced an explanatory diagram setting out how the intelligence cycle works including how officials make use of bulk cable interception.

---

<sup>134</sup> See Report on the final version of the Intelligence and Security Services Act 2017 (27 February 2018): <https://www.ctivd.nl/over-ctivd/documenten/publicaties/2018/02/27/index>; First progress report on the implementation of the Intelligence and Security Services Act 2017 (4 December 2018): <https://www.ctivd.nl/onderzoeken/v/voortgangsrapportage-i> ; Second progress report on the implementation of the Intelligence and Security Services Act 2017 (11 June 2019): <https://www.ctivd.nl/onderzoeken/v/voortgangsrapportage-ii> Upcoming: third and fourth progress reports on the implementation of the Intelligence and Security Services Act 2017: October 2019 and May 2020.

<sup>135</sup> Upcoming review reports on bulk interception available at: <https://www.ctivd.nl/onderzoeken>.

<sup>136</sup> 'CTIVD 2018 Annual report', Official English Translation, page 21, available at: <https://english.ctivd.nl/documents/annual-reports/2019/06/20/index>.

<sup>137</sup> 'The Wiv 2017, A critical contemplation of the Act in an international context', Lotte Houwing, citing Parliamentary Papers II 2017/18, 34588, 69.

<sup>138</sup> <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2018:7459>.

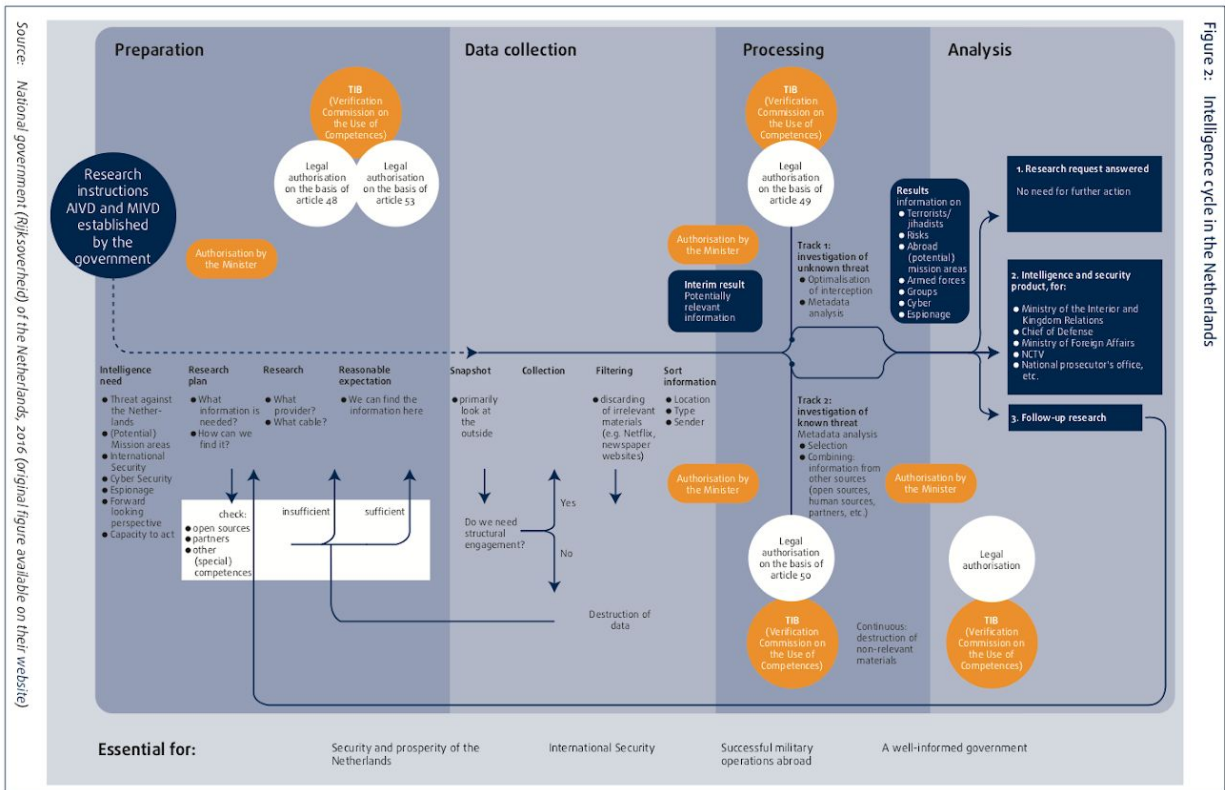


Figure 2: Intelligence cycle in the Netherlands

Fig. 10: [Image available on page 31 of this translated report from the national government of the Netherlands](#)<sup>139</sup>

## Finland

In Finland, a multi-year reform process has resulted in new legislation which officially confirms bulk cable interception and sets out a framework to regulate its use. Similar to the Netherlands, bulk cable interception was historically prohibited, and thus there was significant public debate prior to the passage of legislation. The Finnish Government undertook detailed comparative analysis of models used by other countries which are regulating bulk cable interception.<sup>140</sup> It ultimately adopted a model that draws on both the U.K. and Swedish approaches, according to the former UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin.<sup>141</sup>

<sup>139</sup> Originally provided by the national government of the Netherlands, and translated by the EU Fundamental Rights Agency. See: 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Volume II: field perspectives and legal update', European Union Agency for Fundamental Rights (2017) available at: <https://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega>.

<sup>140</sup> 'Guidelines for developing Finnish intelligence legislation - working group report', Ministry of Defence (2015) available at:

[https://www.defmin.fi/files/3144/GUIDELINES\\_FOR\\_DEVELOPING\\_FINNISH\\_INTELLIGENCE\\_LEGISLATION.pdf](https://www.defmin.fi/files/3144/GUIDELINES_FOR_DEVELOPING_FINNISH_INTELLIGENCE_LEGISLATION.pdf).

<sup>141</sup> Twitter exchange between Martin Scheinin and Eric Kind

<https://twitter.com/MartinScheinin/status/1161205910091509760>.

As of June 2019, the *Civilian Intelligence Act* and *Military Intelligence Act* came into force in Finland.<sup>142</sup> The two Acts officially confirm bulk interception and provide for new powers enabling the Finnish Security Intelligence Service and Finnish Defence Intelligence Agency to conduct “technical gathering and processing of information on data communications crossing the Finnish border.”<sup>143</sup>

The *Military Intelligence Act* regulates telecommunications intelligence<sup>144</sup> using technologically neutral terms, but the explanations<sup>145</sup> to the government bill expressly highlight “cable-transmitted data communications”<sup>146</sup> as the primary focus of the collection [CCM - 2.a], as well as the need to target “specific fibre within a cable.”<sup>147</sup> The *Military Intelligence Act* describes “[o]btaining information from the communications flow [...] based on the use of search parameters.”<sup>148</sup> [CCM - 2.b] A request for court authorization must specify “the search parameters or categories of search parameters to be used in the collection of data and the reasons for them.”<sup>149</sup>

The Finnish Military Intelligence Centre performs the interception of telecommunications cables on behalf of the Finnish Security Intelligence Service. However, in a similar fashion to the Swedish approach, the *Military Intelligence Act* requires telecommunications operators to “redirect the data communications flow of the part specified in the permit to the Military Intelligence Centre.”<sup>150</sup>

## Other Countries

A number of other countries have officially confirmed they either currently undertake bulk cable interception or wish to in the future, including France, Canada, South Africa, and Norway. While there is

<sup>142</sup> Thanks to Martin Scheinin who provided the core analysis, and unofficial translation of the Finnish approach to bulk cable interception. All errors are the author’s own.

<sup>143</sup> ‘*Civilian Intelligence Act to improve Finland’s national security*’, Ministry of the Interior (2019) available at: [https://intermin.fi/en/article/-/asset\\_publisher/sivilitiedustelulaki-parantaa-suomen-kansallista-turvallisuutta](https://intermin.fi/en/article/-/asset_publisher/sivilitiedustelulaki-parantaa-suomen-kansallista-turvallisuutta).

<sup>144</sup> §68 Military Intelligence Act 2019.

<sup>145</sup> In Finland explanations accompanying government bills are a source of law as preparatory works that are frequently relied upon by courts as representing the intent of the legislator.

<sup>146</sup> See explanations from the sub-chapter on data communications intelligence supporting the Government Bill 203/2017 ‘*As the overwhelming majority of data communication flows between Finland and foreign countries passes through optic fibres inside cables used for transferring data, data communications intelligence would in practice be directed at cable-transmitted data communications.*’

<sup>147</sup> See explanations of §69 supporting the Government Bill 203/2017 ‘*According to the provision, the connection to a specific fibre within a cable that crosses Finland’s border would be executed by the executor of a connection with the assistance of a data transferer designated in the permission obtained from a court pursuant to Sections 64, 66 and 68.*’

<sup>148</sup> See §68 Military Intelligence Act: ‘*Intelligence directed at data communications of a State actor (1) The Military Intelligence Centre may, by ways of automated processing of data crossing Finland’s borders within communications networks obtain information concerning the data communications of a State actor considered important for an intelligence task and process communications of a State actor. Obtaining information from the communications flow is based on the use of search parameters.*’ The two Acts permit targeting of more than just ‘state actors’ but have different search rules.

<sup>149</sup> §69(3)(2) Military Intelligence Act.

<sup>150</sup> See §72 Military Intelligence Act, ‘*Performing the connection required for processing of technical data and for communications data intelligence.*’

official confirmation, these countries have yet to publish significant materials around their practices at similar levels to countries above. It is expected that more information will slowly become public in these countries as oversight bodies engage with these new powers (as in the case of Canada), or as the parliamentary debate continues (as in the case of Norway). It should be noted that there will be other countries that undertake such practices that have not been identified during the research for this report. There will also be countries undertaking the practice in secret.

**France.** A close reading of the French *Intelligence Act 2015* leads to the conclusion that it provides for powers to undertake bulk cable collection. The legal regime authorizes powers to undertake “surveillance of international communications” which is defined as “communications emitted from or received abroad.”

The *Intelligence Act 2015* permits the Prime Minister to designate which telecommunications network infrastructure should be subjected to large-scale interception<sup>151</sup> [CCM - 2]. Safeguards provide for, post collection, the deletion of communications that originate and end within France.<sup>152</sup> Powers provide for “non-individualized exploitation of intercepted connection data”<sup>153</sup> which is best understood as bulk metadata analysis. Bulk content exploitation can take place if the Prime Minister issues an authorization.<sup>154</sup>

**Canada.**<sup>155</sup> The *CSE Act* avows and provides powers for Canadian intelligence agencies to undertake bulk cable interception. However, beyond the language in the Act, there is little other official information published setting out technical or operational details.<sup>156</sup> More details may be provided in the course of litigation that is already underway.<sup>157</sup> The *CSE Act* explicitly notes that one of the CSE’s authorized activities includes the “acquisition of information through the global information infrastructure, including unselected information”<sup>158</sup>, [CM - 2] and defines “unselected” as: “with respect to information, means that the information is acquired, for technical or operational reasons, without the use of terms or

<sup>151</sup> Article L.854-2-1 French Intelligence Act 2015.

<sup>152</sup> Article L. 854-1 French Intelligence Act 2015.

<sup>153</sup> Article L. 854-1 French Intelligence Act 2015.

<sup>154</sup> For a fuller analysis, of what recent French intelligence legislation covers, see ‘*Internet Surveillance in France’s Intelligence Act*’, (2016) Félix Tréguer, available at: <https://halshs.archives-ouvertes.fr/halshs-01399548/document>.

<sup>155</sup> Thanks to Tamir Israel who provided the core analysis how the Canadian regime approaches bulk cable interception.


<sup>156</sup> A more detailed analysis of the *CSE Act*, with citations to government as well as other sources, can be found in: Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson & Ronald Deibert, “Analysis of the *Communications Security Establishment Act* and Related Provisions in Bill C-59 (*An Act respecting national security matters*)”, December 2017, *The Citizen Lab & CIPPIC*, [https://cippic.ca/uploads/20171218-C59\\_CSE\\_Analysis-1.0.pdf](https://cippic.ca/uploads/20171218-C59_CSE_Analysis-1.0.pdf); Lex Gill, Tamir Israel & Christopher Parsons, “Government’s Defence of Proposed CSE Act Falls Short”, (Jan. 29, 2018), *The Citizen Lab & CIPPIC*, [https://cippic.ca/uploads/201801-CSE\\_Act\\_Defences\\_Fall\\_Short.pdf](https://cippic.ca/uploads/201801-CSE_Act_Defences_Fall_Short.pdf).

<sup>157</sup> *British Columbia Civil Liberties Association v. Canada (Attorney General)*, Statement of Claim T-2210-14, Federal Court of Canada, <https://bccla.org/wp-content/uploads/2014/12/20141027-CSEC-Statement-of-Claim.pdf>.


<sup>158</sup> § 26(2)(b) CSE Act.



criteria to identify information of foreign intelligence interest.”<sup>159</sup> There are some limitations on targeting any Canadian or person in Canada.<sup>160</sup>



**South Africa.** Legal filings<sup>161</sup> from the South African intelligence agencies<sup>162</sup> set out the government's view on bulk interception. A common affidavit argues that “bulk surveillance is an internationally accepted method of strategically monitoring transnational signals in order to screen them for certain cue words or key phrases”<sup>163</sup> and that “it is basically done through the tapping or recording of transnational signals, including, in some cases, undersea fibre optic cables.”<sup>164</sup> Collection is informed by the “National Intelligence Priorities which include imminent and anticipated threats [...] organised crime, [and] food security, water security and illicit financial flows.”<sup>165</sup> Once collected, “fully automated” systems “extract Intercept Related Information” before it is stored and backed up. The case is being brought by the amaBhungane Centre for Investigative Journalism.<sup>166</sup> Privacy International and Right2Know have intervened to the case as friends of the court.<sup>167</sup>



**Norway.** Finally, Norway does not currently undertake bulk cable collection, but a new *Intelligence Service Act*<sup>168</sup> proposes new powers for bulk cable collection.<sup>169</sup> The details of the proposal is likely to be amended, but currently it provides for the automatic collection and storage for 18 months of all metadata that crosses Norway’s borders [CCM - 2], with judicial warrants needed to collect content, and judicial warrants also needed to search and view either metadata or content. Oversight will be provided by the Norwegian Parliamentary Oversight Committee on Intelligence and Security Services.

---

<sup>159</sup> § 2 CSE Act.

<sup>160</sup> While much in the *CSE Act* prohibits the CSE from directing its activities, including its unselected interception activities, at any Canadian or person in Canada (§ 22(1)) including prohibiting the CSE from directing some of its activities at “information infrastructure that is in Canada,” (§ 22(2)(a)), this prohibition does not apply to the CSE’s unselected information acquisition powers.

<sup>161</sup> Common Affidavit of Minister of State Security, the Office for Interception of Centres, the National Communications Centre and the State Security Agency (2019) available at: [https://www.dropbox.com/sh/w6y420sbgll850r/AADvfgsuv9Nda5Qoe9oJX5i6a?dl=0&lst=&preview=170719\\_spies+answering+affidavit.pdf](https://www.dropbox.com/sh/w6y420sbgll850r/AADvfgsuv9Nda5Qoe9oJX5i6a?dl=0&lst=&preview=170719_spies+answering+affidavit.pdf) [hereinafter referred to as South Africa common affidavit].

<sup>162</sup> This includes the Minister of State Security, the Office for Interception of Centres, the National Communications Centre and the State Security Agency.

<sup>163</sup> §130 South Africa Common Affidavit.

<sup>164</sup> §131 South Africa Common Affidavit.

<sup>165</sup> §135 South Africa Common Affidavit.

<sup>166</sup> amaBhungane Centre for Investigative Journalism NPC and Stephen Partick Sole v. Minister of Justice and Correctional Services and 9 other respondents, Case no: 25978/17, High Court of South Africa, Gauteng Division, Pretoria.

<sup>167</sup> ‘Privacy International and Right 2 Know Campaign amicus curiae’, (2019) available at: <https://privacyinternational.org/legal-action/amabhungane-and-sole-case-south-africa>.

<sup>168</sup> Norwegian Intelligence Service Act available at: <https://www.regjeringen.no/contentassets/556459ec77bd448f828af034dd573e11/horingsnotat---forslag-til-ny-lov-om-etterretningstjenesten.pdf>.

<sup>169</sup> ‘Annual Report 2018’, Norwegian Parliamentary Oversight Committee on Intelligence and Security Services (2018), available at: [https://eos-utvalget.no/wp-content/uploads/2019/05/eos\\_annual\\_report\\_2018.pdf](https://eos-utvalget.no/wp-content/uploads/2019/05/eos_annual_report_2018.pdf).

## Conclusion

Far from being a secret, bulk cable interception is now officially confirmed in a number of countries.

In the U.K., Sweden, the Netherlands, and Germany there is significant information placed in the public domain by the government, creating a reasonably complete picture of the practice. This includes every key stage of bulk interception, including collection, extraction, filtering, selection, storage, and analysis.

In Sweden, the Netherlands, and Germany, officials publicly acknowledge a substantial amount of technical detail; much more than in the United States. Reviews into selection criteria, the application of selectors to bulk systems, and even the sharing of selectors from other countries have all been examined and publicly reported on.

Different countries have arrived at a position of public confirmation via a variety of routes. Some countries like Sweden, the Netherlands, and Norway chose to publicly debate whether their intelligence agencies should engage in such activities before actually deploying the technology. Others, like the U.K., began in secret, and only officially confirmed bulk cable interception a decade after it began.

What is clear, in all cases, is that there is no suggestion that official confirmations of the existence of bulk cable interception in any way endangers national security or undermines the effectiveness of signals intelligence agencies.

Indeed, it must be remembered that the U.K. is the U.S.'s closest and oldest international intelligence partner, and both the U.K. and another close U.S. intelligence partner, Sweden, have both officially confirmed the practice — in Sweden's case more than 13 years ago.<sup>170</sup>

Courts in the U.K., the Netherlands, Germany, and Sweden have all heard claims related to bulk interception, with the responding government officially confirming the practice rather than hiding behind a veil of secrecy. U.S. courts are equipped to hear such challenges as well, but the U.S. government has interposed claims of secrecy to thwart such judicial examination. If intelligence agencies act unlawfully in conducting bulk interception, then the courts should be able to make that assessment, and notify those who were unlawfully spied on. If U.K. courts have been able to make that assessment of illegality, and notify claimants who were unlawfully spied on, without endangering national security, then the U.S. courts should be able to do so as well.

---

<sup>170</sup> See *'The National Security Agency – An Enduring and Vital Partnership'*, GCHQ, (2018) available at: <https://www.gchq.gov.uk/news/joint-statement>; and "A new organization has joined the 'Five Eyes' and is seen as the largest cooperating partner to [the U.K.'s] GCHQ outside the English-speaking countries – and that is Sweden," [Duncan] Campbell". "Sweden sits on pipeline of intelligence 'gold'", The Local, (2013) available at: <https://www.thelocal.se/20130906/50114>.



Given the clear evidence from nine countries that official confirmation of bulk cable interception has been undertaken without apparent risk to national security, it is time for the U.S to revisit its position and provide more transparency on these practices.

## Annex I - Acronyms

CSE - Canadian Communications Security Establishment  
 AIVD - Dutch General Intelligence and Security Service  
 BND - German Federal Intelligence Service  
 CCM - Core Conceptual Model  
 CTIVD - Dutch Review Committee on the Intelligence and Security Services  
 FRA - Swedish National Defense Radio Establishment  
 GCHQ - U.K. Government Communications Headquarters  
 MIVD - Dutch Military Intelligence and Security Service  
 NSA - US National Security Agency  
 RIPA - U.K. Regulation of Investigatory Powers Act  
 WIV - Dutch Intelligence and Security Services Act

## Annex II - Legislation

Country	Statute	Published	English translation
U.K.	Investigatory Powers Act 2016	<a href="https://services.parliament.uk/bills/2015-16/investigatorypowers.html">https://services.parliament.uk/bills/2015-16/investigatorypowers.html</a>	
U.K.	Regulation of Investigatory Powers Act 2000	<a href="https://www.legislation.gov.uk/ukpga/2000/23/contents">https://www.legislation.gov.uk/ukpga/2000/23/contents</a>	NA
U.K.	Interception of Communications Code of Practice	<a href="https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf">https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf</a>	
Sweden	Signals Intelligence Act 2008	<a href="https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2008717-om-signalspaning-i_sfs-2008-717">https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2008717-om-signalspaning-i_sfs-2008-717</a>	<a href="https://cdt.org/files/2019/09/14-e-GOVT-Annex-6.pdf">https://cdt.org/files/2019/09/14-e-GOVT-Annex-6.pdf</a>

Germany	G10 Law	<a href="https://www.gesetze-im-internet.de/g10_2001/">https://www.gesetze-im-internet.de/g10_2001/</a>	<a href="http://www.ennir.be/sites/default/files/pictures/GermanLawsgoverningParliamentaryControlofIntelligenceActivities.pdf">http://www.ennir.be/sites/default/files/pictures/GermanLawsgoverningParliamentaryControlofIntelligenceActivities.pdf</a> [Official]
Germany	BND Law	<a href="https://www.gesetze-im-internet.de/bndg/">https://www.gesetze-im-internet.de/bndg/</a>	
France	Intelligence Act 2015	<a href="https://www.legifrance.gouv.fr/affichCode.do;jsessionid=BF72E2C1162C7C49D52DE78D65BEF5B4.tpdila07v_2?idSectionTA=LEGISCTA000030934655&amp;cidTexte=LEGITEXT000025503132&amp;dateTexte=20160309">https://www.legifrance.gouv.fr/affichCode.do;jsessionid=BF72E2C1162C7C49D52DE78D65BEF5B4.tpdila07v_2?idSectionTA=LEGISCTA000030934655&amp;cidTexte=LEGITEXT000025503132&amp;dateTexte=20160309</a>	<a href="https://wiki.laquadrature.net/French_Intelligence_Laws">https://wiki.laquadrature.net/French_Intelligence_Laws</a> [Unofficial]
Canada	CSE Act 2018	<a href="https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/third-reading/enH3105">https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/third-reading/enH3105</a>	NA
Netherlands	Wiv 2017	<a href="https://wetten.overheid.nl/BWBR0039896/2018-05-01">https://wetten.overheid.nl/BWBR0039896/2018-05-01</a>	
Finland	Civilian Intelligence Act 2019	<a href="https://www.finlex.fi/fi/laki/ajantasa/2019/20190709">https://www.finlex.fi/fi/laki/ajantasa/2019/20190709</a>	
Finland	Military Intelligence Act 2019	<a href="https://www.finlex.fi/fi/laki/ajantasa/2019/20190711">https://www.finlex.fi/fi/laki/ajantasa/2019/20190711</a>	
Norway	Proposed Intelligence Service Act	<a href="https://www.regjeringen.no/contentassets/556459ec77bd448f828af034dd573e11/horingsnotat---forslag-til-ny-lov-om-etterretningstjenesten.pdf">https://www.regjeringen.no/contentassets/556459ec77bd448f828af034dd573e11/horingsnotat---forslag-til-ny-lov-om-etterretningstjenesten.pdf</a>	