

# Mass Surveillance and the Right to Privacy

# Privacy International & the Right to Privacy

## Guide to International Law and Surveillance

Stakeholder Report  
Universal Periodic Review  
30th Session - Colombia

### The Right to Privacy in Colombia

### The Right to Privacy in South Africa

### The Right to Privacy in the Islamic Republic of Pakistan

## NECESSARY & PROPORTIONATE


The International Principles on the Application of Human Rights to Communications Surveillance (the “Necessary and Proportionate Principles” or “13 Principles”) show how existing human rights law applies to modern digital surveillance. Drafted by a global coalition of civil society, privacy and technology experts in 2013, they have been endorsed by over 600 organizations and over 270,000 individuals worldwide.

**The UN Special Rapporteur on the right to privacy** 9

How NGOs can interact with the UN Special Rapporteur on the right to privacy

**Other UN Special Rapporteurs**

How NGOs can interact with the

**Human Rights Committee**

How NGOs can interact with the

**Universal Periodic Review**

How NGOs can interact with the Universal Periodic Review 14

## HOW TO TALK ABOUT THE RIGHT TO PRIVACY AT THE UN

IN THE

Supreme Court of the United States



IN THE MATTER OF A WARRANT TO SEARCH A  
CERTAIN EMAIL ACCOUNT CONTROLLED AND MAINTAINED  
BY MICROSOFT CORPORATION

UNITED STATES OF AMERICA,

—v—

MICROSOFT CORPORATION,

*Petitioner,*

*Respondent*

ON WRIT OF CERTIORARI TO THE UNITED STATES  
COURT OF APPEALS FOR THE SECOND CIRCUIT

BRIEF OF PRIVACY INTERNATIONAL,  
HUMAN AND DIGITAL RIGHTS ORGANIZATIONS,  
AND INTERNATIONAL LEGAL SCHOLARS AS  
*AMICI CURIAE* IN SUPPORT OF RESPONDENT

## EUROPE'S TOP HUMAN RIGHTS COURT WILL CONSIDER LEGALITY OF SURVEILLANCE EXPOSED BY EDWARD SNOWDEN

Ten organizations – including Privacy International, the American Civil Liberties Union, and Amnesty International – are taking up the landmark case against the U.K. government in the European Court of Human Rights (pictured above). In a [115-page complaint](#) released on Thursday, the groups allege that “blanket and indiscriminate” surveillance operations carried out by British spy agencies in collaboration with their U.S. counterparts violate privacy and freedom of expression rights.

- A. International Human Rights Law Recognizes a Fundamental Right to Privacy in Personal Electronic Data ..
- B. Numerous Foreign Governments Have Developed Specific Legal Regimes to Protect Individuals' Data from Unwanted Intrusion .....
- C. Foreign Governments Have Entered into Specific Agreements to Regulate International Data Transfers and Law Enforcement Data Requests .....

# 10 Human Rights Orgs. v. United Kingdom

- FACTUAL HISTORY
- PROCEDURAL HISTORY
- LEGAL ARGUMENTS
- JUDGMENT
- IMPLICATIONS FOR MASS SURVEILLANCE PROGRAMS

# Factual History: Mass Interception

## GCHQ taps fibre-optic cables for secret access to world's communications

**Exclusive: British spy agency collects and stores vast quantities of global email messages, Facebook posts, internet histories and calls, and shares them with NSA, latest documents from Edward Snowden reveal**

One key innovation has been GCHQ's ability to tap into and store huge volumes of data drawn from fibre-optic cables for up to 30 days so that it can be sifted and analysed. That operation, codenamed Tempora, has been running for some 18 months.

GCHQ and the NSA are consequently able to access and process vast quantities of communications between entirely innocent people, as well as targeted suspects.



# Factual History: Mass Interception

## How Bulk Interception Works

Governments conduct bulk interception by tapping high capacity fibre optic cables, which carry the world's internet communications. The TAT-14, for example, is a transatlantic cable system with a transmission capacity of 3.15 terabits per second, or approximately 34 petabytes per day. To put that number into perspective, 1 petabyte is roughly equivalent to 2 billion cat photos.\*

\*1 cat photo = 500 kilobytes (KB)

~~PRIVACY~~  
INTERNATIONAL



### 1 Interception

Capturing a signal (a stream of packets) from the cable.

### 2 Extraction

Copying the stream, directing it into a storage space, and reassembling packets.

### 3 Filtering

Separating out information using "selectors" – for example, email or IP addresses, "all calls from country x to country y", search engine queries containing particular words, or even broader descriptors.

### 4 Storage

Retaining information in databases for analysis.

### 5 Analysis

Querying, reading, examining, data-mining, or otherwise analysing information stored in databases.

### 6 Dissemination

Distributing the results of analysis to other people, organisations or agencies.



Foreign governments may also be granted access to information at any stage of the bulk interception process.

# Factual History: Mass Interception

The Intercept\_

## PROFILED

From Radio to Porn, British Spies Track Web Users' Online Identities

One system builds profiles showing people's web browsing histories. Another analyzes instant messenger communications, emails, Skype calls, text messages, cellphone locations, and social media interactions. Separate programs were built to keep tabs on "suspicious" Google searches and usage of Google Maps.

The agency used a sample of nearly 7 million metadata records, gathered over a period of three months, to observe the listening habits of more than 200,000 people across 185 countries, including the U.S., the U.K., Ireland, Canada, Mexico, Spain, the Netherlands, France, and Germany.

Black Hole contains data collected by GCHQ as part of bulk "unselected" surveillance, meaning it is not focused on particular "selected" targets and instead includes troves of data indiscriminately swept up about ordinary people's online activities. Between August 2007 and March 2009, GCHQ [documents say](#) that Black Hole was used to store more than 1.1 trillion "events" — a term the agency uses to refer to metadata records — with about 10 billion new entries added every day.

# Factual History: Intelligence Sharing

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



## SKYNET: Applying Advanced Cloud-based Behavior Analytics

A Collaborative Project  
by S2I, R6, T12, T14,  
SSG, and S22

Presenters:  
S2I51  
R66F



Derived From: NSA/CSSM 1-52  
Dated: 20070108  
Declassify On: 20370401

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

# Factual History: Intelligence Sharing



## MUSCULAR (DS-200B)

TOP SECRET//COMINT//REL-USA,GBR

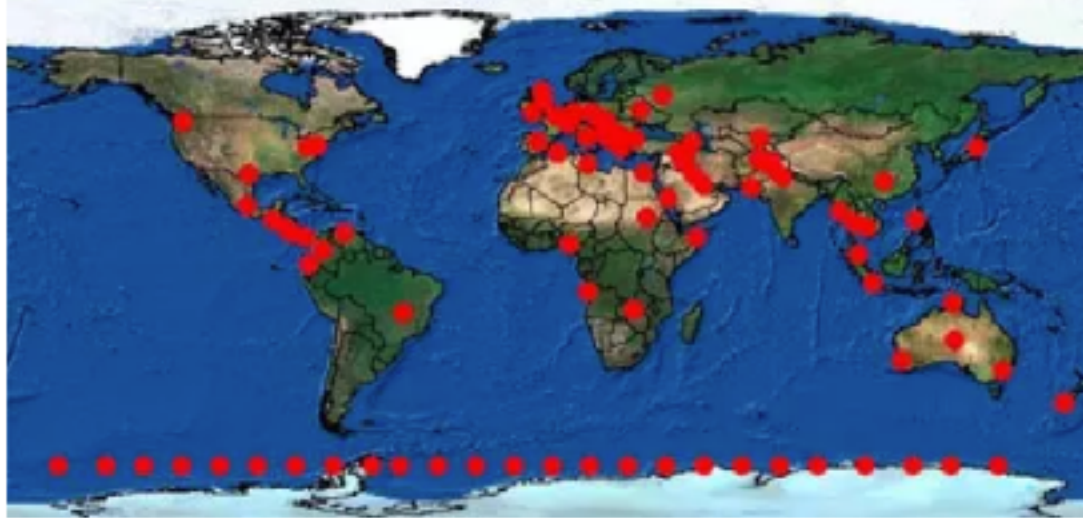
- Operational July 2009
- (S//REL USA,GBR) Large international access located in United Kingdom
- Four TURMOIL T16s at 2.5Gb each - total ingest 10Gb
- LPTs installed May 2010 increase ingest to 20Gb
- Tasking worked cooperatively with GCHQ counterparts
- Partner to assume total control/responsibility for systems
- IP Subnet promotion in place, VoIP in the works

TOP SECRET//COMINT//REL-USA,GBR

## Goal

The goal of this training is to get you familiar with basic HTTP traffic and understand how to target and exploit it using X-KEYSCORE

## Where is X-KEYSCORE?



## I want to....



- So let's put the cookie query all together...
  - Between Marina and XKS, I should have an idea of all the accounts..

- Results pulling on dg8q0cd4u0li4 as a Search Value

Search File	Search Value	Match Type	Link to File
dg8q0cd4u0li4	dg8q0cd4u0li4	YAHOO	dg8q0cd4u0li4
dg8q0cd4u0li4	dg8q0cd4u0li4	YAHOO	dg8q0cd4u0li4
dg8q0cd4u0li4	dg8q0cd4u0li4	YAHOO	dg8q0cd4u0li4

- Plus my Marina results

ACTIVE	USER ID	COOKIE
dg8q0cd4u0li4	seen with machine ID dg8q0cd4u0li4	dg8q0cd4u0li4
dg8q0cd4u0li4	seen with machine ID dg8q0cd4u0li4	dg8q0cd4u0li4
dg8q0cd4u0li4	seen with machine ID dg8q0cd4u0li4	dg8q0cd4u0li4

RESULTS: Three users on the a computer..

TOP SECRET//COMINT//REL-USA,GBR,NZL

# Procedural History

- July 2013: Privacy International filed complaint before UK Investigatory Powers Tribunal
  - Joined by 9 NGOs: American Civil Liberties Union, Amnesty International, Bytes for All, Canadian Civil Liberties Association, Egyptian Initiative for Personal Rights, Hungarian Civil Liberties Union, Irish Council for Civil Liberties, Legal Resources Centre, Liberty
- December 2014-June 2015: 3 judgments
- March 2015: Application challenging judgments before European Court of Human Rights
- April-September 2016: First round of submissions by Government and applicants
- July 2017: Case joined with *BBW et al. v UK & BIJ & Alice Ross v. UK*
- September 2017: Second round of submissions by applicants
- November 2017: Oral hearing
- September 2018: Judgment

# Challenging Mass Interception

## Article 8 of the European Convention on Human Rights

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

### “in accordance with law”

- basis in domestic law
- accessible
- foreseeable

### “necessary in a democratic society”

“[The Court] must also ascertain whether the requested interception meets the requirement of ‘necessary in a democratic society’...including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means.”

*Zacharov v. Russia (2016)*

# Evolution of Surveillance Safeguards

*Weber & Saravia v. Germany (2006)*

“minimum safeguards that should be set out in statute law in order to avoid abuses of power”

- nature of offences that may give rise to surveillance
- categories of people who may be subject to surveillance
- temporal limits on surveillance
- procedure for examining, using and storing data obtained
- precautions when disseminating data
- circumstances for destroying data

*Szabo & Vissy v. Hungary (2016)*

“[T]he rule of law implies... that an interference ...should be subject to an effective control which should normally be assured by the judiciary...”

*Zacharov v. Russia (2015)*

“[the authority] must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or...acts endangering national security.”

“As soon as notification can be carried out without jeopardising the purpose of the restriction ..., information should...be provided, to the persons concerned.”

# Challenging Mass Interception

## UK Government Observations to ECtHR (April 2016)

- “may in principle result in the interception of ‘substantial quantities of communications...contained in ‘bearers’ carrying communications to many countries”
- “may in principle authorise the interception of internal communications insofar as that is necessary in order to intercept the external communications”

## Government Witness Statement to Investigatory Powers Tribunal (May 2014)

“A person conducting a Google search...[m]aking a post on Facebook, or ‘tweeting’ on Twitter” communicates with a server outside of the UK and therefore makes an ‘external communication’...”

# Challenging Intelligence Sharing

## Compare:

(1) GCHQ intercepts a text between A and B, both located in London, as it leaves the UK on a transatlantic fiber optic cable.

VS.

(2) NSA taps a transatlantic fiber optic cable and gives GCHQ access to raw intercept material (including the text between A and B).

VS.

(3) NSA intercepts the text between A and B as it arrives in the US on a transatlantic fiber optic cable and provides it - solicited or unsolicited - to GCHQ.

# Challenging Intelligence Sharing

1. A request may only be made by the Intelligence Services to the government of a country or territory outside the United Kingdom for unanalysed intercepted communications (and associated communications data), otherwise than in accordance with an international mutual legal assistance agreement, if either:

a. a relevant interception warrant under the Regulation of Investigatory Powers Act 2000 ("RIPA") has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the communications at issue because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the Intelligence Services to obtain those communications; or

b. making the request for the communications at issue in the absence of a relevant RIPA interception warrant does not amount to a deliberate circumvention of RIPA or otherwise contravene the principle established in *Padfield v. Minister of Agriculture, Fisheries and Food* [1968] AC 997 (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the Intelligence Services to obtain those communications.

For these purposes a "relevant RIPA interception warrant" means either (i) a s8(1) warrant in relation to the target at issue; (ii) a s8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" (within the meaning of s8(4)(b) of RIPA) covering the target's communications, together with an appropriate s16(3) modification (for individuals known to be within the British Islands); or (iii) a s8(4) warrant and accompanying certificate which includes one or more "descriptions of intercepted material" covering the target's communications (for other individuals). The reference to a "warrant for interception, signed by a Minister" being "already in place" in the ISC's Statement of 17 July 2013 should be understood in these terms. (Given sub-paragraph (b), and as previously submitted in open, a RIPA interception warrant is not as a matter of law required in all cases in which unanalysed intercepted communications might be sought from a foreign government.)

2. Where the Intelligence Services receive unanalysed intercepted communications content and associated communications data from the government of a country or territory outside the United Kingdom (whether solicited or unsolicited), those communications and communications data are – pursuant to internal "arrangements" – subject to the same internal rules and safeguards as selected

communications content and related communications data that are obtained directly by the Intelligence Services as a result of interception under RIPA. For these purposes, "selected communications content" means communications content resulting from interception under a s8(1) warrant, or from the selection processes that are applied, pursuant to s16 of RIPA, to communications obtained under a s8(4) warrant.

3. Those of the Intelligence Services that receive unanalysed intercepted material and related communications data from an interception under a s8(4) warrant have internal "arrangements" that require a record to be created, explaining why access to the unanalysed intercepted material is required, before an authorised person is able to access such material pursuant to s16 of RIPA.

4. The internal "arrangements" of those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s8(4) warrant specify (or require to be determined, on a system-by-system basis) maximum retention periods for different categories of such data which reflect the nature and intrusiveness of the particular data at issue. The periods so specified (or determined) are normally no longer than two years, and in certain cases are significantly shorter (intelligence reports that draw on such data are treated as a separate category, and are retained for longer). Data may only be retained for longer than the applicable maximum retention period where prior authorisation has been obtained from a senior official within the particular Intelligence Service at issue on the basis that continued retention of the particular data at issue has been assessed to be necessary and proportionate (if the continued retention of any such data is thereafter assessed to no longer meet the tests of necessity and proportionality, such data are deleted). As far as possible, all retention periods are implemented by a process of automated deletion which is triggered once the applicable maximum retention period has been reached for the data at issue. The maximum retention periods are overseen by, and agreed with, the Interception of Communications Commissioner.

5. The intelligence services' internal "arrangements" under the Security Service Act 1989 / the Intelligence Services Act 1994 and s15-16 of RIPA are periodically reviewed to ensure that they remain up-to-date and effective. Further, the Intelligence Agencies are henceforth content to consider, during the course of such periodic reviews, whether more of those internal arrangements might safely and usefully be put into the public domain (for example, by way of inclusion in a relevant statutory code of practice).

## UK-US surveillance regime was unlawful 'for seven years'

Regulations governing access to intercepted information obtained by NSA breached human rights laws, according to Investigatory Powers Tribunal

# Judgment Highlights: Mass Interception

- Within a state's "margin of appreciation" - i.e. does not per se violate Article 8
- UK program unlawful because:
  - Lacked sufficient oversight over:
    - Selection of "bearers"
    - Filtering and selection of comms using "selectors" and "search criteria"
  - Lacked no safeguards over:
    - Interception and processing of communications-related metadata

# Judgment Highlights: Metadata

“[T]he Court is not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content. For example, the content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient. The related communications data, on the other hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with...” (§ 356)

# Judgment Highlights: Intelligence Sharing

“As with any regime which provides for the acquisition of surveillance material, the regime for the obtaining of such material from foreign Governments must be ‘in accordance with the law’...Furthermore, it must be proportionate to the legitimate aim pursued, and there must exist adequate and effective safeguards against abuse. In particular, the procedures for supervising the ordering and implementation of the measures in question must be such as to keep the ‘interference’ to what is ‘necessary in a democratic society’.” (§422)

# Judgment Highlights: Intelligence Sharing

“Indeed...as States could use intelligence sharing to circumvent stronger domestic surveillance procedures and/or any legal limits which their agencies might be subject to as regards domestic intelligence operations, a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques’.” (§423)

# Judgment and Investigatory Powers Act 2016

## MASS INTERCEPTION

- No oversight of selection of “bearers”
- No oversight of use of “selectors” and “search criteria”
- No safeguards for communications-related metadata

## INTELLIGENCE SHARING

- Intelligence sharing confined to “receipt” of information



# A New Era of Mass Surveillance is Emerging Across Europe

Journalists go to court over Germany's 'unrestrictive' surveillance laws

Press groups have argued that Germany's surveillance laws are unconstitutional as they allow foreign reporters to be monitored. The case is raising awareness on social media under the slogan "No trust, no news."

## France's sweeping surveillance law goes into effect

*Constitutional Council broadly approves controversial law, despite protests from civil liberties groups*

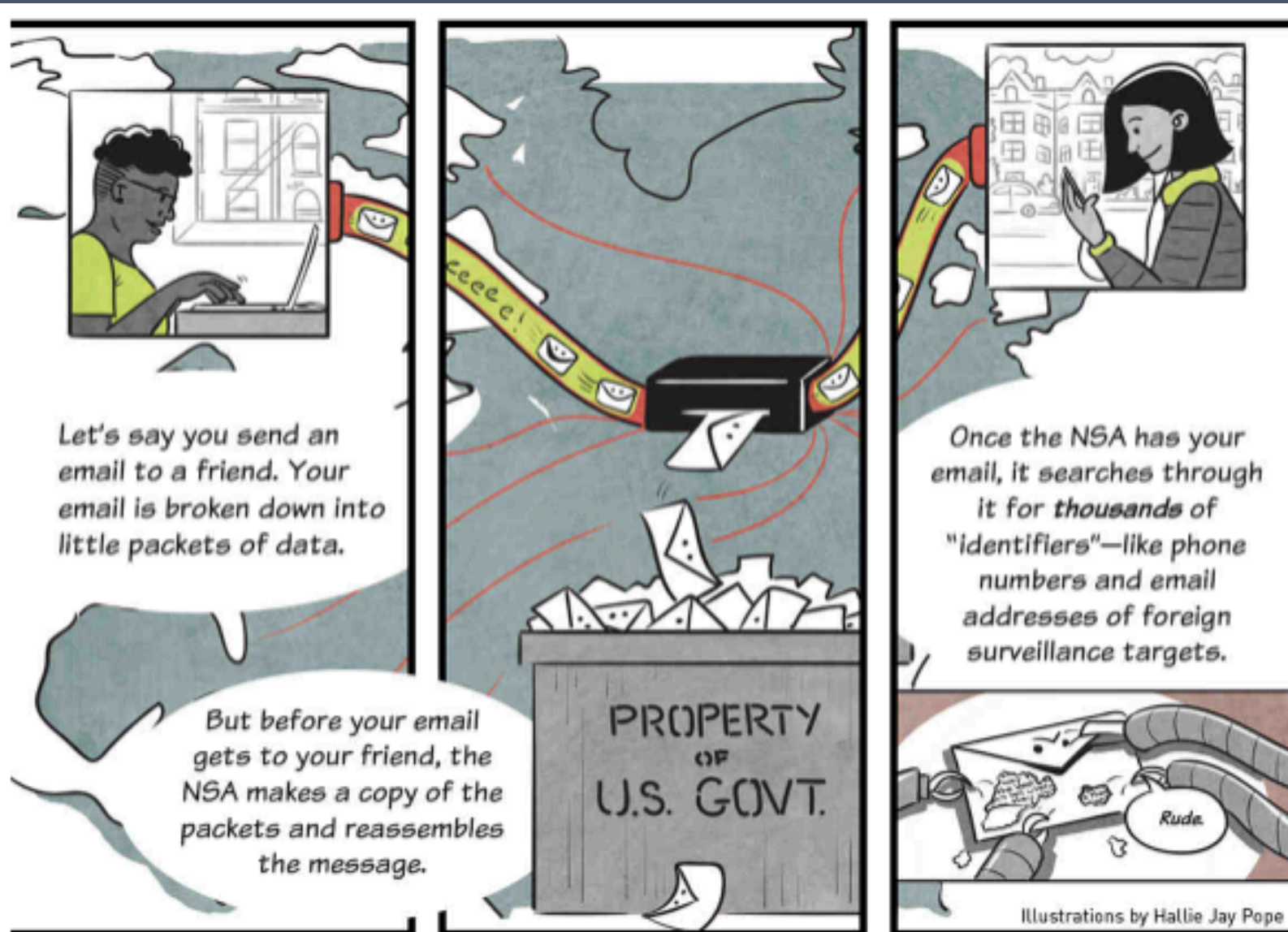
## European Rights Group Criticizes Poland's Surveillance Law

Bill giving Polish police greater powers to spy on foreigners also advances in parliament

**Austria creates new agency with unprecedented surveillance powers**

**Italy: Anti-terrorism decree to strengthen government surveillance**

# WIKIMEDIA V. NSA - CHALLENGE TO UPSTREAM SURVEILLANCE UNDER THE FISA AMENDMENTS ACT



# Approved SIGINT Partners



## Second Parties

Australia  
Canada  
New Zealand  
United Kingdom

## Coalitions/Multi-lats

AFSC  
NATO  
SSEUR  
SSPAC

## Third Parties

Algeria	Israel	Spain
Austria	Italy	Sweden
Belgium	Japan	Taiwan
Croatia	Jordan	Thailand
Czech Republic	Korea	Tunisia
Denmark	Macedonia	Turkey
Ethiopia	Netherlands	UAE
Finland	Norway	
France	Pakistan	
Germany	Poland	
Greece	Romania	
Hungary	Saudi Arabia	
India	Singapore	

PRIVACY  
INTERNATIONAL

## Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards



April 1, 2011

“Our research suggests that most countries around the world lack domestic legislation governing intelligence sharing.”

**Art. 45 GDPR**

# **Transfers on the basis of an adequacy decision**

**“2. When assessing...adequacy...the Commission shall, in particular, take account of...:**

- a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred...”**