



KEEPING THE INTERNET  
OPEN • INNOVATIVE • FREE

[www.cdt.org](http://www.cdt.org)

1634 I Street, NW  
Suite 1100  
Washington, DC 20006

P +1-202-637-9800  
F +1-202-637-0968  
E [info@cdt.org](mailto:info@cdt.org)

## EUROPEAN COURT TO DECIDE WHETHER MASS SURVEILLANCE IS CONSISTENT WITH HUMAN RIGHTS: BIG BROTHER WATCH V. UK

April 3, 2014

In September 2013 a group of non-governmental organizations and activists led by Big Brother Watch filed a challenge in the European Court of Human Rights (ECtHR) against surveillance activities conducted by the UK government as disclosed by former National Security Agency contractor Edward Snowden. Today, CDT and PEN American Center applied to the ECtHR to intervene in the case because of its significant implications for human rights on the Internet. The ECtHR addresses violations of the European Convention on Human Rights (ECHR). According to Article 46 of the Convention, the Court's decisions are binding on its 47 signatory countries. It could rule in the near future that mass surveillance violates international human rights law.

### I. Facts, Claims, and Context

The application, filed by Big Brother Watch, Open Rights Group, English PEN and Dr. Constanze Kurz of the Computer Chaos Club, claims that UK government surveillance programs violate Article 8 of the ECHR by monitoring communications, and by gathering communications information, without sufficient justification.<sup>1</sup> Article 8 guarantees the right to privacy.<sup>2</sup> In early January the ECtHR accepted the case,<sup>3</sup> and requested a response by the UK Government to three key questions by May 2. The ECtHR also gave priority to the case, employing a rarely invoked process that allows it to fast track the review based on the "importance and urgency of the issues raised," (ECtHR Rule 41) reflecting a strong interest by the Court in responding to recently revealed government surveillance activities.

---

<sup>1</sup> The full application can be found here:

[http://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/libe/dv/bbw\\_org\\_ep\\_ck\\_v\\_uk\\_bbw\\_org\\_ep\\_ck\\_v\\_uk\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/bbw_org_ep_ck_v_uk_bbw_org_ep_ck_v_uk_en.pdf). A witness statement by Doctor Ian Brown, available here: [https://www.privacynotprism.org.uk/assets/files/privacynotprism/IAN\\_BROWN-FINAL\\_WITNESS\\_STATEMENT.pdf](https://www.privacynotprism.org.uk/assets/files/privacynotprism/IAN_BROWN-FINAL_WITNESS_STATEMENT.pdf), and a witness statement of EFF Legal Director Cindy Cohn, available here: [https://www.privacynotprism.org.uk/assets/files/privacynotprism/CINDY\\_COHN-FINAL\\_WITNESS\\_STATEMENT.pdf](https://www.privacynotprism.org.uk/assets/files/privacynotprism/CINDY_COHN-FINAL_WITNESS_STATEMENT.pdf).

<sup>2</sup> Article 8 of the ECHR states: "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 wellbeing 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."

<sup>3</sup> For full letter of the ECtHR accepting the case, putting forward its questions to be addressed, and providing its Statement of Facts for the case, see [https://www.privacynotprism.org.uk/assets/files/privacynotprism/letter\\_from\\_ecthr\\_to\\_uk\\_gov.pdf](https://www.privacynotprism.org.uk/assets/files/privacynotprism/letter_from_ecthr_to_uk_gov.pdf).

This case has the potential to be profound in the ongoing surveillance debate. Unlike U.S. courts, which have refrained from addressing global surveillance programs due to obstacles to demonstrating legal standing, the ECtHR is likely to decide this case on its merits (further discussion below). Thus, there is a realistic possibility of a high profile court with binding legal authority over 47 European countries ruling in the near future that mass surveillance is illegal and violates international human rights law. A ruling by the ECtHR that the surveillance programs at issue violate the European Convention on Human Rights could propel some European countries to significantly reform their surveillance laws.

The legal challenge focuses on three surveillance programs that Big Brother Watch and the other applicants claim are implicated in the UK's violations of ECHR Article 8. First is the U.S. government's PRISM program, through which the U.S. National Security Agency obtains electronic communications content to, from or about more than 100,000 foreign targets without judicial authorization. Second is the U.S. government's UPSTREAM program, which involves the mass collection of data from fiber optic cables carrying Internet traffic in and out of the U.S. so it can later be searched. Although these programs are operated by the U.S. government, the applicants claim the UK government has used information obtained through PRISM and UPSTREAM, gathering UK citizens' communications content absent ministerial approval in situations where warrants would have to be obtained if such interceptions were to be conducted directly under authority of the UK government.

Third is the TEMPORA program. This program – similar to the NSA's UPSTREAM program in the U.S. – is a UK government program that involves tapping the fiber cables carrying Internet traffic to scan and analyze all electronic data that goes in or out of the UK. This program is operated by the Government Communications Headquarters (GCHQ), a UK surveillance agency responsible for providing signals intelligence to the government and military.

## II. Legal Issues

In anticipation of its review of these programs, the ECtHR put forth the following three questions to be addressed by the parties:

1. Can the applicants claim to be victims of violations of their rights under Article 8?
2. Have the applicants done all that is required of them to exhaust domestic remedies?
3. In the event that the application is not inadmissible on grounds of non-exhaustion of domestic remedies, are the acts of the UK intelligence services “in accordance with the law” and “necessary in a democratic society” within the meaning of Article 8 of the Convention?

The first two questions go to the matter of “admissibility.” Admissibility limits whom may apply to the ECtHR and on what grounds their application may be founded, based on rules set forth in the ECHR. Two of the most important criteria limiting admissibility are that applicants must be victims of a violation, and that applicants must have exhausted all domestic remedies. The other main issues regarding admissibility – whether an application is redundant as to a prior request, whether an application is under review by another international court, and whether the ECtHR has jurisdiction to hear the case – are unlikely to be of any concern for this case.

Addressing the first question will be relatively straightforward, and presents far less of an obstacle to the applicants than would the corresponding inquiry under U.S. law. While U.S. courts require a showing of actual harm by parties challenging government activity – a prerequisite that has largely constrained domestic challenges to surveillance pursuant to Section 702 of FISA, notably in *Clapper v. Amnesty* – the ECtHR has ruled on many occasions that the “mere existence” of surveillance law which could potentially affect applicants is sufficient for the applicants to claim to be victims of a violation of Article 8 rights (*Klass v. Germany*; *Association for European Integration and Human Rights v. Bulgaria*; *Lordachi v. Moldova*).

The second question – exhaustion – is also unlikely to prevent the Court from assessing the merits. In *Kennedy v. The UK*, the ECtHR ruled in 2010 that the Investigatory Powers Tribunal (IPT) – an entity within the UK Executive branch where the government requested Big Brother Watch file its complaint – cannot provide an effective judicial remedy for privacy violations where the sufficiency of the regulatory and oversight regime (of which that tribunal is part) is at issue. Nonetheless, the UK government has filed a letter with the Court asking it to find that the applicants failed to exhaust domestic remedies by seeking relief first at the IPT. It argued that other entities had filed such an application, putting at issue surveillance similar to that under challenge in the present proceedings. Tellingly, the UK did not even mention the *Kennedy* case.

The final question – whether the surveillance activities are “in accordance with the law” and “necessary in a democratic society” – is likely to be the most contentious, and require the greatest focus of the Court. The applicants contend that surveillance must be necessary and proportionate, in accordance with adequate laws, and subject to independent warranting and transparent oversight processes. They argue that none of these requirements currently apply in the UK. According to the applicants, the relevant statute – the Regulation of Investigatory Powers Act (RIPA) – does not regulate the sharing of foreign surveillance data, fails to impose sufficient safeguards on collection of “external” communications (communications to which all parties are outside the UK), and empowers the very ministers whose agencies benefit from surveillance to sign the warrants that authorizes it. They also argue that the commissioners and parliamentary committees that provide surveillance oversight are ineffective in light of the scale of surveillance activities recently disclosed and those authorities’ responses to the disclosures.

In order to prevail, the applicants must convince the ECtHR that the surveillance programs at issue are either not in accordance with the law, or not necessary in a democratic society or that, even within these limitations, they represent a disproportionate interference with citizens’ right to privacy. Encouragingly, the ECtHR directed the parties to discuss *Weber and Saravia v. Germany*, *Liberty v. the United Kingdom*, and *Lordachi v. Moldova* – which all condemn conducting broad surveillance activities in secret – in responding to this question. According to these cases, in order to be “in accordance with law,” surveillance must be apparent based on the law (i.e., citizens have “an adequate indication” of the general circumstances in which the law permits surveillance – a limited foreseeability test), and contain limits on purpose, duration, retention and use of information collected.

The Court’s assessment will be based on a balancing of government needs against the scale of the surveillance activities at issue. The government is likely to rely heavily the threat posed by terrorism to tip the scales. The applicants will focus on the indiscriminate nature of the surveillance because the ECtHR has previously required (notably in *Weber and Saravia*) that some limits exist on the scope of surveillance, even in responding to legitimate threats.

### III. Interventions

The ECtHR permits outside individuals and entities to “intervene” in cases (similar to filing an amicus brief in the U.S. system) in order to provide information or legal analysis in addition to that provided by the parties. Interveners assist the court on assessing issues falling within the intervener’s expertise. CDT and the PEN American Center filed an application to intervene today. We sought leave to intervene in order to help the Court consider, in connection with its evaluation of the merits of the case:

- The broader impact of the surveillance at issue on the willingness of writers, reporters and human rights defenders to communicate with others, engage in research and writing, and exercise the right of free expression, based in part on [PEN American’s Chilling Effects report](#);
- The impact on Internet communications of surveillance avoidance policy proposals that the surveillance at issue has engendered, including mandatory data localization;
- The extent to which measures President Barack Obama announced on January 17, 2014, including Presidential Decision Directive #28, impact the Article 8 rights of the applicants; and
- How UK surveillance law measures up to the laws of other nations in terms of human rights, based in part on [CDT’s report on Systematic Government Access to Personal Data](#).

If the Court grants our request for permission to intervene, the intervention itself will be due a few weeks later. CDT and PEN American are represented [“instructed” in UK parlance] on a *pro bono* basis by UK barristers: [Hugh Southey QC](#) from Matrix Chambers leading [Can Yeginsu](#) and [Anthony Jones](#) from 4 New Square Chambers.

For more information: contact CDT’s Greg Nojeim, Senior Counsel and Director of the Project on Freedom, Security and Technology ([gnojeim@cdt.org](mailto:gnojeim@cdt.org)), or Jake Laperruque, Privacy, Surveillance and Security Fellow ([jake@cdt.org](mailto:jake@cdt.org)). At PEN American, contact Katy Glenn Bass, Deputy Director of Free Expression Programs ([kglennbass@pen.org](mailto:kglennbass@pen.org)).