WRITTEN SUBMISSION

In the case of

Big Brother Watch and others v. The United Kingdom
Application no. 58170/13

1. Introduction and summary

1.1 These written submissions are made on behalf of Asociația pentru Tehnologie și Internet, Stichting Bits of Freedom, Digitalcourage e.V., Digital Rights Ireland Limited, Digitale Gesellschaft e.V., European Digital Rights, Electronic Frontier Finland – Effi ry, Föreningen för digitala fri- och rättigheter, Initiative für Netzfreiheit, IT-Politisk Forening, La Quadrature du Net, Panoptykon Foundation and Verein für Internet-Benutzer Österreichs ("**EDRi and others**") pursuant to leave granted by the President of the First Section of the European Court of Human Rights (the "**Court**").

1.2 These European organisations are all active in the field of human rights in the information society, and in particular the right to privacy and to freedom of communication. They are closely involved in policy debates on a national and European level regarding internet surveillance and human rights and have specialised expertise in this area.

1.3 The present case is a crucial opportunity for the Court to revise its framework for the protection of personal data in view of technological developments in the field of surveillance technology. In this submission, EDRi and others want to focus on one particular aspect of this framework: the protection afforded to "metadata" or "traffic data" compared to "content" of communications.[1] In summary, EDRi and others argue that:

i. "Metadata" and "traffic data" provide information about the behavior of persons under surveillance (these kinds of data in this submission will be called "**behavioral data**"). This behavioral data can paint a very detailed picture of a person – even more detailed than what could be constructed on the basis of 'content'. And it can be far more intimate, as will be further explained below. That is why intelligence agencies consider this information to be very valuable. And moreover, decisions with a grave impact, such as the killing of people, are based

[1] In their request for leave to intervene, EDRi and others also offered to discuss the 'chilling effect' of surveillance on their work. As it is understood that this issue will also be discussed by the Center for Democracy and Technology, it was subsequently decided to not discuss it in this intervention.

on the analysis of behavioral data. Meanwhile, vast pools of behavioral data are generated daily, most of it unwittingly.

ii. In *Malone v. The United Kingdom* (no. 8691/79) and *P.G. & J.H. v. The United Kingdom* (no. 44787/98), the Court made an explicit distinction between "content" and behavioral data, suggesting that behavioral data should be afforded less protection. Governments built their surveillance programs on that distinction, arguing that the collection and analysis of behavioral data needed fewer safeguards.

iii. However, the sensitivity of the behavioral data generated in enormous quantities every day, combined with the advances in surveillance capabilities, call for the adoption by the Court of a new framework for assessing behavioral data-related interferences. In particular, different degrees of protection afforded to personal data should not be based on the arbitrary and irrelevant distinction between "content" and other types of data. Instead, these degrees of protection should be based on (i) the nature of the data and (ii) the inferences which can be drawn from this data. The more sensitive the nature of the data or the inferences which can be drawn from it, the more protection should be afforded to this data. This analysis should not only take into account the inferences which can be drawn from data "in isolation" or only relating to one person, but also when combined with other data to which a Government has access to or in theory could gain access to, and the advanced analytical capabilities which are available, or in theory come or will be available.

2. "Metadata" and "traffic data" provide information about behavior

2.1 The terms "metadata" and "traffic data" are not very precisely delineated. "Metadata" is often used to describe information *about* a communication: when someone called, who was called, the duration of the call, etc. "Traffic data" has a similar but more technical meaning, often used to describe information generated in the course of making a call, such as the antenna towers used to set up a connection, or the IP-addresses used between two points of communication. The Court in the past used the term "metering data" to describe something similar but more related to billing: a process which, according to the Court "involves the use of a device (a meter check printer) which registers the numbers dialled on a particular telephone and the time and duration of each call" (*Malone*, § 83).

2.2 It is important to note that, regardless of their exact scope, these terms relate to data generated using a *variety of* services, such as mobile telephony services (this would include antenna towers used, unique identifier of device, unique identifier of SIM-card), mobile internet services (this would include antenna towers used at a particular moment, unique identifier of device, IP-addresses, websites visited) and email services (this would include from:- and to: emailadresses and time of sending). But this term could also be understood to include the address books of all contacts of a certain user

sent automatically over the internet by messaging services such as WhatsApp. As will be argued below, this could even include data generated by standalone devices such as thermostats.

2.3 As mentioned above, in this submission the term "**behavioral data**" will be used to describe these kinds of data, without attempting to precisely draw the boundaries with "content" (as it will be argued that the distinction has become irrelevant). The term behavioral data is chosen to reflect the relevance of the data: it is data about the *behavior* of persons. Or in the words of a cryptography expert pointing out the sensitivity of what he calls "metadata":[2]

> "There's more to privacy than just the sounds of our voices: Content may be what we *say*, but metadata is about what we actually *do*."

3. Behavioral data can paint a detailed and intimate picture of a person

Behavioral data allows for mapping of social networks

3.1 Behavioral data can be quite revealing. It can firstly be used to map social networks. Note that these networks can be built on the basis of communication data ('who was communicating with whom'), but also on the basis of locational proximity ('who was where'). The latter technique was applied by the National Security Agency ("**NSA**") in the CO-TRAVELER programme. The NSA according to the Washington Post "gathered nearly 5 billion records a day on the whereabouts of cellphones around the world", and "[u]sing these vast location databases, the NSA applies sophisticated analytics techniques to identify what it calls co-travelers — unknown associates who might be traveling with, or meeting up with a known target".[3]

Behavioral data allows for location tracking

3.2 Related to this, it can be used to track the location of persons. The tracking in itself can already be quite invasive. However, one can also *infer* sensitive information from location data, such as religion (being in the proximity of a mosque at prayer times), health (visiting an abortion clinic), sexual orientation (visiting a gay bar) and political affiliation (being at a demonstration). But also more mundane data can be considered quite private: at what time someone is at home, goes to work, is on vacation, etc.

---

[2] See Matt Blaze, "Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)", *Wired* 19 June 2013, to be found at: http://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/

[3] See B. Gellmann and A. Soltani, "How the NSA is tracking people right now", *Washington Post* 4 December 2013, to be found at: https://www.washingtonpost.com/apps/g/page/world/how-the-nsa-is-tracking-people-right-now/634/ and "NSA tracking cellphone locations worldwide, Snowden documents show", *idem*, to be found at: https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html

Behavioral data allows for internet browsing tracking

3.3 Behavioral data can furthermore be used to track internet browsing habits. By way of illustration, GCHQ has the capability with a program called KARMA POLICE to (i) identify all 'visible' (i.e. intercepted) persons who visited a certain website, and (ii) observing which websites a certain person visited. The way GCHQ uses this capability is quite revealing:[4]

> "[The GCHQ analysts] zeroed in on any stations found broadcasting recitations from the Quran, such as a popular Iraqi radio station and a station playing sermons from a prominent Egyptian imam named Sheikh Muhammad Jebril. They then used KARMA POLICE to find out more about these stations' listeners, identifying them as users on Skype, Yahoo, and Facebook. The summary report says the spies selected one Egypt-based listener for "profiling" and investigated which other websites he had been visiting. Surveillance records revealed the listener had viewed the porn site Redtube, as well as Facebook; Yahoo; YouTube; Google's blogging platform, Blogspot; the photo-sharing site Flickr; a website about Islam; and an Arab advertising site".

Behavioral data allows for the mapping of communication patterns

3.4 And even the simple act of communicating can be used to *infer* sensitive information. Some communication endpoints (such as telephone numbers or email-addresses) are used for a single purpose – i.e. support for victims of domestic violence or rape, addicts, people struggling with their sexual identity – and a communication with that endpoint in itself already reveals very private information.[5] Sometimes, communication *patterns* can be sensitive: for example calling one's boyfriend, calling the abortion clinic, then calling one's parents and then calling the abortion clinic again. Sometimes, communication *frequency* can reveal information, such as whether a relationship is ending and another one might be starting.

Behavioral data allows for insight into people a person interacts with

3.5 Often, most of the attention in a privacy analysis relates to the "primary" person generating the data. It should be noted, however, that behavioral data also provides information on people this person associates or interacts with, such as information on their relationship.

---

[4] See R. Gallagher, "Profiled: from radio to porn, British spies track web users' online identities", *The Intercept* 25 September 2015, to be found at: https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/

[5] See also the declaration by Professor Edward Felten of 23 August 2013 in the case between *ACLU and others v. James Clapper and others*, § 40, to be found at: https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf

The level of detail of behavioral data is magnified when analysed on a large scale

3.6 The information which can be inferred from behavioral data only increases as the amount of data accessible to intelligence agencies grows and the technologies enabling such inference become more advanced. What might be relatively insensitive data when only relating to one person over a period of a few days, may allow for more sensitive inferences if relating to hundreds of thousands of people over hundreds of days. In the words of Professor Edward Felten:[6]

> "The analyst uses metadata about many individuals to discover patterns of behavior that are indicative of some attribute of an individual. The analyst can then apply these patterns to the metadata of an individual user, to infer the likely attributes of that user. In this way, the effect of collecting metadata about one individual is magnified when information is collected across the whole population."

3.7 The European Court of Justice in *Digital Rights Ireland v. Minister for Communications & Others* (cases C-293/12 and C-594/12, 8 April 2014) confirmed this with regard to a relatively limited amount of behavioral data (§ 27):

> "Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."

3.8 An illustration of this can be found in two case studies where persons subjected their own behavioral data to an analysis. In one, an employee of one of the parties to this intervention, Bits of Freedom, provided investigators with one week of his location data, search history and email- and phone data (except for content). The investigators were able to piece together a detailed profile of him.[7] In another one, a German politician mapped similar data, illustrating the privacy impact visually.[8]

3.9 All in all, behavioral data can paint a very detailed picture of a person and the people he or she interacts with – even more detailed than what could be constructed on the basis of content. And it can be far more intimate. As noted in the International Principles on the Application of Human Rights to Communications Surveillance: "metadata provides a window into nearly every action in modern life, our mental states,

---

[6] *Idem*, § 63.

[7] See D. Tokmetzis, "How your innocent smartphone passes on almost your entire life to the secret service", *Bits of Freedom* 30 July 2014, to be found at: https://www.bof.nl/2014/07/30/how-your-innocent-smartphone-passes-on-almost-your-entire-life-to-the-secret-service/

[8] See K. Biermann, "Betrayed by our own data", *Zeit Online* 10 March 2011, to be found at: http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz

interests, intentions, and our innermost thoughts".[9] Or in the words of Stewart Baker, the general counsel of the NSA:[10]

> "Metadata absolutely tells you everything about somebody's life, […] If you have enough metadata you don't really need content…. [It's] sort of embarrassing how predictable we are as human beings."

4. Intelligence agencies also consider behavioral data to be valuable

4.1 It is no surprise then, that intelligence agencies also consider behavioral data to be very valuable. In an internal memo, where the Director of National Intelligence is requested to establish a "US Intelligence Community-wide communications metadata sharing structure", the director of the NSA notes that (emphasis added):[11]

> "SIGINT metadata is a *vast, rich source of information* to build community collaboration and target knowledge and the emerging intelligence based target social network analysis discipline."

5. People may even be killed on the basis of behavioral data

5.1 Not only is behavioral data sensitive: the decisions which are *based on* behavioral data can also be far-reaching. These may lead to imprisonment, rendition and – in extreme cases – even killing.[12] A former drone operator for the US military's Joint Special Operations Command (JSOC) who also worked with the NSA was summarized by *The Intercept* as saying:[13]

> "the agency often identifies targets based on controversial metadata analysis and cell-phone tracking technologies. Rather than confirming a target's identity with operatives or informants on the ground, the CIA or the U.S. military then orders a strike based on the activity and location of the mobile phone a person is believed to be using."

---

[9] See International Principles on the Application of Human Rights to Communications Surveillance, final version May 2014, to be found at: https://en.necessaryandproportionate.org/text

[10] As quoted in A. Rusbridger, "The Snowden Leaks and the Public", *New York Review of Books* 21 November 2013, to be found at: http://www.nybooks.com/articles/2013/11/21/snowden-leaks-and-public/

[11] See *Decision Memorandum for the DNI on ICREACH*, published on *The* I*ntercept* on 25 August 2014, to be found at: https://theintercept.com/document/2014/08/25/decision-memorandum-dni-icreach/

[12] It was noted in an internal NSA document from 2005 published on The Intercept on 25 August 2014 that the use of communications metadata "has been a contribution to virtually every successful rendition of suspects and often, the deciding factor", to be found at https://theintercept.com/document/2014/08/25/metadata-sharing-memorandum-2005/. See also R. Gallagher, "The Surveillance Engine", *The Intercept* 25 August 2014, to be found at https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/

[13] See J. Scahill and G. Greenwald, "The NSA's Secret Role in the U.S. Assassination Program", *The Intercept* 10 February 2014, to be found at: https://theintercept.com/2014/02/10/the-nsas-secret-role/

5.2 Or in the words of Michael Hayden, ex-director of the NSA and the CIA: "We kill people based on metadata".[14] This not only illustrates the grave impact the use of behavioral data potentially has, but also the evidentiary value and accuracy apparently attributed by intelligence services to this data.

6. Vast pools of behavioral data are generated every day, often unwittingly

6.1 Meanwhile, vast pools of behavioral data are generated every day – and most of it is generated unintentionally. For example, a mobile phone automatically connects periodically to an antenna tower of a telecommunications provider in the vicinity. The owner of that phone doesn't intend this to happen, though – and he is probably not even aware that it happens.

6.2 Related to this, the generation of most behavioral data is unavoidable.[15] The owner of a mobile phone cannot choose to *not* use the antenna tower of a telecommunications provider to set up a phone call. It cannot avoid to have its email messages routed through a number of internet connection and email providers: this is an integral element of the transport of email messages.

6.3 While the prior examples were related to data generated in the course of communicating, it is important to note that a continuous stream of behavioral data is also generated when *not* communicating. For example, apps on a phone may send periodic updates to a server, and this in itself already generates behavioral data. This is compounded by the fact the generation of certain behavioral data is continuous: for example, mobile phones are always on, and will be generating behavioral data throughout the day, even when their owners are sleeping.

6.4 And while all examples above relate to smartphone-related behavioral data, a massive increase in this kind of data is expected as a result of many more devices becoming connected to the internet. This development is often called the "internet of things", pointing to the generation of data by navigation devices on cars, "smart watches", security cameras, baby monitors, thermostats, etc. These all create data about their users, most of which will not be considered "content", but very sensitive nevertheless.

6.5 Thus, instead of "content" being considered the most central and sensitive element of (communications-related) privacy, it should be concluded that "content" is a mere

---

[14] As quoted in D. Cole, "We Kill People Based on Metadata", *New York Review of Books* 10 May 2014, to be found at: http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/

[15] See the declaration by Professor Edward Felten of 23 August 2013 in the case between *ACLU and others v. James Clapper and others*, to be found at: https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf.

drop of data compared to the vast pool of behavioral data generated by each person every day – often unwittingly, and not all related to communications.

7. The Court made a distinction between behavioral data and content

7.1 In 1984, the Court in *Malone* for the first time made a distinction between behavioral data and content (§ 84):

> "By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8 (art. 8). The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone."

7.2 The Court clarified this view in 2001 in *P.G. & J.H.*, § 42:

> "The Court notes, however, that metering, which does not per se offend against Article 8 if, for example, done by the telephone company for billing purposes, is by its very nature to be distinguished from the interception of communications which may be undesirable and illegitimate in a democratic society unless justified (see Malone, cited above, pp. 37-38, §§ 83-84)."

7.3 The Court mostly focused on whether there was an *interference* with the right to privacy when "metering" data was involved, and it did not explicitly discuss the question of necessity and proportionality. It even calls the numbers dialled 'an integral element' of phone communications. Meanwhile, it did *suggest* that these data should be afforded less protection.

8. Governments built their surveillance programs on this distinction

8.1 Governments based the limits of their surveillance activities with regard to behavioral data on the assumption that this type of data was afforded lower protection. For example, GCHQ according to *The Guardian* in an internal memo noted:[16]

> "There are extremely stringent legal and policy constraints on what we can do with content, but we are much freer in how we can store metadata. Moreover, there is obviously a much higher volume of content than metadata. […] For these reasons,

[16] See E. MacAskill et al., "How does GCHQ's internet surveillance work?", *The Guardian* 21 June 2013, to be found at: http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work

> metadata feeds will usually be unselected – we pull everything we see; on the other hand, we generally only process content that we have a good reason to target."

8.2 Similarly, in a presentation on "Events analysis" (the term used by GCHQ for behavioral data), GCHQ noted that this data is "less intrusive than communications content", concluding in the following bullet that "authorisation **not** needed for individuals in the UK" (emphasis in original).[17]

8.3 It is also noted in the International Principles on the Application of Human Rights to Communications Surveillance officially launched at the UN Human Rights Council in Geneva in September 2013 that "[d]espite the vast potential for intrusion into an individual's life and the chilling effect on political and other associations, laws, regulations activities, powers, or authorities often afford communications metadata a lower level of protection [than content] and do not place sufficient restrictions on how they can be subsequently used by States".[18]

9. The Court should thus adopt a new framework for assessing behavioral data-related interferences

9.1 The Court's considerations on behavioral data in *Malone* and *P.G. and J.H* are decades old. In *Malone,* the internet and mobile phones did not yet exist. In *P.G. and J.H.*, the public was not yet aware of the advanced surveillance capabilities available to intelligence services at that time, while these capabilities have only increased since then. Furthermore, the suggestion of the Court that this data can be used for billing purposes does not apply anymore either: as most subscriptions are flat-fee, bills are not based on the amount of communications which took place, and behavioral data is not relevant for invoicing in any other way. Thus, the Court's considerations in these cases do not translate well to the present circumstances.

9.2 The Review Group on Intelligence and Communications Technologies commissioned by the President of the United States in its report on the NSA's surveillance already considers the assumption questionable that "meta-data does not seriously invade individual privacy."[19] It continues:

---

[17] See presentation on Events Analysis, published by *The Intercept* on 25 September 2015, to be found at: https://theintercept.com/document/2015/09/25/events-analysis/ and accompanying article R. Gallagher, "Profiled: from radio to porn, British spies track web users' online identities", *The Intercept* 25 September 2015, to be found at: https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/

[18] See International Principles on the Application of Human Rights to Communications Surveillance, final version May 2014, to be found at: https://en.necessaryandproportionate.org/text

[19] The President's Review Group on Intelligence and Communications Technologies , *The NSA Report: Liberty and Security in a Changing World*, Princeton University Press 2014, pp. 72-73, also to be found at: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

> "In a world of ever more complex technology, it is increasingly unclear whether the distinction between "meta-data" and other information carries much weight. The quantity and variety of meta-data have increased. […] Although the legal system has been slow to catch up with these major changes in meta-data, it may well be that, as a practical matter, the distinction itself should be discarded."

9.3 The Court itself recently in *Szabó and Vissy v. Hungary* (no. 37138/14, § 70) underlined that the threat to privacy posed by the possibility of "Governments to acquire a detailed profile […] of the most intimate aspects of citizens' lives […] must be subjected to very close scrutiny both on the domestic level and under the Convention". It continued that "[t]he guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices".

9.4 In conclusion, EDRi and others argue that the Court should adopt a new framework under Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms in order to address the ever-growing threat of surveillance. In this framework, different degrees of protection afforded to personal data should not be based on the arbitrary and irrelevant distinction between "content" and other types of data.

9.5 Instead, the degrees of protection should be based on (i) the nature of the data and (ii) the inferences which can be drawn from this data. The more sensitive the nature of the data or the inferences which can be drawn from it, the more protection should be afforded to this data. This analysis should not only take into account the inferences which can be drawn from data "in isolation" or only relating to one person, but also when combined with other data to which Governments have access to or in theory could gain access to, and the advanced analytical capabilities which are available, or in theory come or will be available.

Ot van Daalen
Project Moore
8 February 2016

Leidsegracht 78
1016 CR Amsterdam
The Netherlands
T 020 5200 891
F 020 5200 871