Submission of evidence to the Intelligence and Security Committee of Parliament - Privacy and Security Inquiry

Mathias Vermeulen*

EXECUTIVE SUMMARY

It is submitted here that the collection, use, retention and dissemination of metadata can be as intrusive into the right to private life as the interception of the content of communications. As a result, statutory laws regulating the collection, use, retention and dissemination of metadata by security agencies would need to include those safeguards that were set out by the European Court of Human Rights in the case Weber and Saravia v. Germany.

EVIDENCE

1. The European Court of Human Rights has recognized that the (1) obtaining, (2) use and (3) further dissemination of (telephone) metadata constitute separate interferences with Article 8 of the European Convention on Human Rights. In P.G and J.H. v. the United Kingdom, both the Court and the UK government acknowledged that the mere "obtaining" by the police of "information relating to the numbers called" on a telephone in a flat interfered with the private lives or correspondence of those who made use of the telephone in the flat or were telephoned from the flat.[1] In an earlier ruling from 1984, the Court accepted that the use of metadata obtained from "metering", a practice that "registers the numbers dialled on a particular telephone and the time and duration of each call" could give rise to "an issue" under article 8. The Court argued further that releasing the records of this metadata to the police without the consent of the subscriber "also" amounted to an interference with a right guaranteed by Article 8.[2]

2. The Court has ruled more generally that the mere storing of information related to a person's private life would amount to an interference of article 8 as well.[3] The Court has embraced a wide definition of a person's private life, saying that it comprises "the right to establish and develop relationships with other human beings". In that context, the Court specifically referred to the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which defines personal data as "any

---

* This evidence is submitted in my personal capacity. I am a Research Fellow at the European University Institute in Florence and a researcher at the Centre for Law, Science and Technology Studies at the Vrije Universiteit Brussels. Between 2008 and 2012 I worked as an assistant of the former United Nations Special Rapporteur on the protection of human rights while countering terrorism. Earlier I worked at the International Commission of Jurists and the Special Procedures Unit of the Office of the High Commissioner for Human Rights in Geneva.

1 ECtHR, P.G. and J.H. v. the United Kingdom, 44787/98, 25/09/2001, §40 - 42.

2 ECtHR, Malone v. the United Kingdom, 8691/79, 02/08/1984, §84.

3 ECtHR, Leander v. Sweden, 9248/81, 26/03/1987, §48.

information relating to an identified or identifiable individual".[4] Importantly, the finding of such an interference is not dependent on the subsequent use of that information.[5]

3. While the Court acknowledges that obtaining, using, retaining and disseminating communications metadata interferes with Article 8, it has argued that this data "by its very nature" has to be distinguished from the interception of the content of communications.[6] The Court has made a similar observation in a case of GPS-surveillance, where it stated that the surveillance via GPS of movements in public places "must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations".[7]

4. As a result of this distinction, the Court until now has argued that the minimum safeguards which are to be set out in statute law in order to avoid abuses of the collection, use, storing and dissemination of metadata have to be less strict than those safeguards that need to be included in laws that regulate the surveillance of the content of communications.[8] In Weber and Saravia v. Germany, the Court summarized the following minimum safeguards that should be set out in statute laws that regulate the interception of communications: a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.[9] Where only metadata is collected, the Court has argued that these strict principles don't necessarily apply. Instead, it must be satisfied that there exist "adequate and effective guarantees against abuse". According to the Court, "this assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law".[10]

5. From 1978 onwards the Court has embraced the notion that the Convention is a "living instrument, which must be interpreted in the light of present-day conditions".[11] One scholar has argued that the importance that is being attached to "present-day conditions" in interpreting the Convention has three features: (1) the Court will very rarely inquire into what the intentions were of the drafters, or what was thought to be acceptable state conduct when the Convention was drafted, (2) the conditions have to be common or shared amongst contracting states and (3) the Court will not assign decisive importance to what the

---

4 ECtHR, Amann v. Switzerland, 27798/95, 16/02/2000, §65.

5 Idem, §69.

6 ECtHR, Malone v. the United Kingdom, 8691/79, 02/08/1984, §84; ECtHR, P.G. and J.H. v. the United Kingdom, 44787/98, 25/09/2001, §42.

7 ECtHR, Uzun v. Germany, 35623/05, 02/09/2010, §65.

8 Idem.

9 ECtHR, Weber and Saravia v. Germany, 54934/00, 29/06/2006, §95.

10 ECtHR, Uzun v. Germany, 35623/05, 02/09/2010, §63. See also ECtHR, P.G. and J.H. v. the United Kingdom, 44787/98, 25/09/2001, §46.

11 ECtHR, Tyrer v. The United Kingdom, 5856/72, 25/04/1978, 31.

respondent state considers to be an acceptable standard in the case at hand.[12] The Court's unwillingness to define the scope of the right to private life, coupled with the evolutive reading of the Convention, has allowed it to take into account a broad range of social, legal and technological developments across the Council of Europe to develop the scope of the right to private life.

6. It is submitted here that the distinction that the Court has made between the intrusiveness of collecting, using and storing metadata and content data is no longer tenable. The falling cost of storing metadata, the increased capacity to mine large sets of metadata, and metadata's ability to create an intimate profile of an individual's life, make the collection and analysis of metadata not less intrusive than the collection and analysis of 'content'. As a result, statutory laws regulating the collection, use, storing and dissemination of metadata by security agencies would need to incorporate the safeguards that the Court summarized in Weber and Saravia v. Germany.[13]

7. The following paragraphs will illustrate how a wide variety of stakeholders, including security experts, civil society organisations, computer scientists and other relevant parties support the main claim of this submission.

8. On the 12th of December 2013, the United States President's Review Group on Intelligence and Communications Technologies presented its report to President Obama. The review group consisted – among others – of a former deputy director of the Central Intelligence Agency, Mr. Michael Morell, and a former counter-terrorism advisor to the US National Security Council, Mr. Richard Clarke. The group stated the following. "The assumption behind the argument that meta-data is meaningfully different from other information is that the collection of meta-data does not seriously invade individual privacy. As we have seen, however, that assumption is questionable. 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. In contrast to the telephone call records at issue in the 1979 case of Smith v. Maryland, today's mobile phone calls create meta-data about a person's location. Social networks provide constant updates about who is communicating with whom, and that information is considered meta-data rather than content. E-mails, texts, voice-over-IP calls, and other forms of electronic communication have multiplied. For Internet communications in general, the shift to the IPv6 protocol is well under way. When complete, web communications will include roughly 200 data fields, in addition to the underlying content. Although the legal system has been slow to catch up with these major changes in meta-data, it may

---

12 George Letsas, "The ECHR as a Living Instrument: Its Meaning and Legitimacy," in *Constituting Europe - The European Court of Human Rights in a National, European and Global Context*, ed. Andreas Follesdal, Birgit Peters, and Geir Ulfstein, Studies on Human Rights Conventions (Cambridge University Press, 2013), 106–141.

13 See also M. Vermeulen, Secrecy trumps location: A short paper on establishing the gravity of privacy interferences posed by detection technologies. Novatica, Special English Edition, 2012/2013, Annual selection of articles, pp.23-25, available at http://www.ati.es/novatica/2013/ASA/NvS2013-23.pdf. Mathias Vermeulen, Paul De Hert, Onze privacy verdient meer bescherming. De Tijd, 14 June 2013.

well be that, as a practical matter, the distinction itself should be discarded".[14]

9. More than 360 civil society organisations signed the International Principles on the application of human rights to communications surveillance in 2013. The preamble of the principles state: "Existing legal frameworks distinguish between "content" or "non-content," "subscriber information" or "metadata," stored data or in transit data, data held in the home or in the possession of a third party service provider. However, these distinctions are no longer appropriate for measuring the degree of the intrusion that communications surveillance makes into individuals' private lives and associations. While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Today, each of these types of information might, taken alone or analysed collectively, reveal a person's identity, behaviour, associations, physical or medical conditions, race, colour, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time, or of all people in a given location, including around a public demonstration or other political event. As a result, all information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public, should be considered to be "protected information", and should accordingly be given the highest protection in law".[15]

10. One of the most thoughtful analyses on the power of metadata was delivered by Professor Edward W. Felten, professor of Computer Science and Public Affairs at Princeton University, before the United States Senate Committee on the Judiciary in October 2013. His analysis should be read in its entirety, but his main point is the following: "Metadata can now yield startling insights about individuals and groups, particularly when collected in large quantities across the population. It is no longer safe to assume that this " summary " or "non - content" information is less revealing or less sensitive than the content it describes. Just by using new technologies such as smart phones and social media, we leave rich and revealing trails of metadata as we move through daily life. Many details of our lives can be gleaned by examining those trails. Taken together, a group's metadata can reveal intricacies of social, political, and religious associations. Metadata is naturally organized in a way that lends itself to analysis, and a growing set of computing tools can turn these trails into penetrating insights. Given limited analytical resources, analyzing metadata is often a far more powerful analytical strategy than investigating content: It can yield far more insight with the same amount of effort".[16] He ends his statement by arguing that "in order to ensure strong

---

[14] Richard Clarke, Michael J.Morell, Geoffrey R. Stone, Cass Sunstein, Peter Swire, Liberty and security in a changing world. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. The White House, 2013, pp.120-121 available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[15] International Principles on the Application of Human Rights to Communications Surveillance, 10 July 2013, available at https://en.necessaryandproportionate.org/

[16] Written Testimony of Edward W. Felten Professor of Computer Science and Public Affairs, Princeton University United States Senate, Committee on the Judiciary Hearing on Continued Oversight of the

oversight of these complex programs, the overseers must have independent access to robust technical expertise".[17]

11. Finally, United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, argued in his report for the Human Rights Council that "when accessed and analysed, even seemingly innocuous transactional records about communications can collectively create a profile of individual's private life, including medical conditions, political and religious viewpoints and/or affiliation, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications alone. By combining information about relationships, location, identity and activity, States are able to track the movement of individuals and their activities across a range of different areas, from where they travel to where they study, what they read or whom they interact with".[18]

Foreign Intelligence Surveillance Act October 2, 2013, p.1., available at http://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf

[17] Idem, p.13.

[18] A/HRC/23/40, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, §42.