Where to after Watson: The challenges and future of data retention in the UK

11 May 2017

SUMMARY OF PROCEEDINGS

A panel of experts examined the implications of the Court of Justice of the European Union's (CJEU) judgment in the *Watson/Tele2 Sverige AB* (Case C-698/15), examining the balance between protecting privacy rights and combatting serious crime, especially in coming post-Brexit years. The event was chaired by Professor Lorna Woods (University of Essex School of Law) and panellists were Max Hill QC (Independent Reviewer of Terrorism Legislation), Dr Nora Ní Loideain (Director of the Information Law and Policy Centre, IALS) and Renate Samson (Chief Executive, Big Brother Watch). A summary of the discussion follows below. The Bingham Centre is grateful to Simmons & Simmons for hosting the event.

Professor Lorna Woods began the event by summarizing *Watson*. Its key ruling was that "general and indiscriminate retention of all traffic and location data" violated Article 15(1) of Directive 2002/58/EC, as interpreted in light of Articles 7, 8, 11, and 52(1) of the Charter of Fundamental Rights of the European Union. Consequently, while access to bulk data may be justified by "the objective of fighting serious crime", it should be subject to prior independent authorisation. People affected by such access to bulk data must also be notified (when the notification will not jeopardise an investigation).

The panel speakers were generally agreed that *Watson*, at face value, represents an increased protection for privacy rights that has been welcomed in many quarters. Max Hill QC observed that *Watson* followed the general "pro-privacy" trend of CJEU decisions, in contrast to the prevailing "pro-law enforcement" trends coming from United Kingdom (UK) courts. Dr Nora Ní Loideain, specifically highlighted that *Watson* duly recognised accessing metadata can be as intrusive to individual privacy rights as accessing the content of particular communications, and thus warrants similar judicial oversight. This equivalence is especially important in an era of rapidly evolving technology that collects big data by default, such as smart homes, fitness trackers and so forth. Renate Samson emphasised that *Watson* also serves as an important conversation starter with citizens about what are and are not justifiable infringements of privacy rights.

Yet, various several issues remain to be resolved. Mr Hill noted that there are at least four pending cases relevant to the issues in *Watson* (such as Privacy International's submission to the European Court of Human Rights, challenging the UK's bulk interception of internet traffic). Their ultimate rulings would thus likely have a bearing on how our understanding and implementation of *Watson* actually occurs. He also suggested that — given the lack of definition for "serious crime" in the judgment — there is little clarity or agreement regarding the extent to which *Watson* data protection requirements apply in the context of national security. This is concerning in light of the multiple crucial roles bulk data can play in preventing crimes like terrorism.

Most importantly, the CJEU has left it to domestic courts to determine whether and to what extent their legislation satisfies the *Watson* ruling. As Dr Ní Loideain pointed out, this arguably leaves national courts as guardians of fundamental rights like privacy. In the UK, then, the outstanding question is whether and to what extent the government will consider *Watson* in relation to the new Investigatory Powers Act 2016 (IPA) (which replaced the expired Data Retention and Investigatory Powers Act 2014 (DRIPA), the legislation that partly triggered the *Watson* ruling).

The IPA has a similar, if not wider provisions for data retention than DRIPA, and no robust requirement of prior independent authorisation of access to bulk data. *Watson* thus casts uncertainty over the validity of powers enshrined in the IPA. The legal landscape is particularly unclear given that CJEU decisions will only technically bind the UK until it has left the EU.

Dr Ní Loideain emphasised there were unsatisfactory reasons as to why the IPA does not currently have an independent statutory body for ex ante oversight. Having such pre-approval for infringements of privacy rights would provide stronger protection than post-facto audits, and help re-instil public trust that governments are acting in compliance with the rule of law. In fact, the *Watson* ruling has opened the door for amendments to the IPA that can serve as world-leading oversight arrangements. This, she argued, would remedy deficiencies in current "double lock mechanism" in the IPA, which essentially privileges executive (rather than judicial) approval of accessing bulk data.

There was some debate regarding the role of companies and government in the conversation about how privacy rights should develop. Mr Hill expressed concern that corporate interests would be contrary to protection of individual privacy protection, so parliamentary officials — as our democratic representatives — should be entrusted to reign supreme in the conversation. Dr Ní Loideain cautioned against putting too much faith in government, as their interests in combatting crime may also lead to infringements of individuals' privacy. The extremely rushed process of passing the IPA 2016, for instance, exemplified government reluctance to create a culture of transparency and accountability regarding bulk data collection and access. The Home Secretary's recent statements to limit end-to-end encryption on social media services like WhatsApp was also cited to show the government's poor appreciation of the rights at stake in the debate. After a wide-ranging question and answer sessions, the event concluded with the speakers affirming the desirability of greater public participation in the privacy protection debate.

Victoria Wicks, Bingham Centre Volunteer Researcher
May 2017