The Lack of Evidence for Supporting Increased Data Retention

https://www.e-ir.info/2012/11/13/the-lack-of-evidence-for-supporting-increased-data-retention/

CLEMENT GUITTON, NOV 13 2012

Traffic data can help to identify instigators of cyber attacks, to some extent. In 2003, it led for instance to the identification of a variant of the Blaster worm, a worm that spread to hundred of thousands of computers. The worm engaged in a denial-of-service attack against Microsoft at a specific date, and one of the variant, Blaster.B, also allowed the hacker to take control of the computer. Blaster.B contacted the website www.t33kid.com to register the infected computer, so the hacker could follow the trace of infected computers. The website that contained the source code for various malware led the police to the arrest of the author of this variant. On 15 August 2003, the police started trying to contact the owner of the website. The website was registered under the California Regional Internet, who confirmed that they rented the IP address to Keith Baldwin from a company called SouthO. Baldwin provided leased computer servers, and had rented the IP address allocated to the website to Brian Davis. Baldwin also gave the police Davis' address. On 16 August, the police obtained a warrant and seized the server hosting the website www.t33kid.com, at Davis' place. Davis stated that a user going under the name of 'teekid' operated the website and that he had chatted with him over the Internet Relay Chat a couple of times. As such, Davis had actually recorded his IP address, which he provided to the police. Two days later, on 18 August, the police found another website that 'teekid' probably operated as well, under the address dl.t33kid.com and confirmed the data provided by Davis. The domain name was registered under a real name, Jeff Parson, On 19 August, the police obtained a search warrant for Jeff Lee Parson, who admitted releasing the Blaster.B variant.[1] Parson's worm hit 48,000 computers, totalising damages of $1,2 million.[2] On 28 January 2005, Parson received a sentence of 18-month prison, three years of supervised release with limited access to a computer, and 100 hours of community service.

In the UK, similar legislation exists to retain traffic data. But the UK is now considering a Bill, the Draft Communication Data Bill, to require communications service providers, which includes Internet service providers, to retain all traffic data about their users online behaviours. The current legislation proposal is far broader and its proponent advances argument to support the tackling of all types of crimes (and not only cyber attacks). The Bill could have many devastating effects, from creating a surveillance society to infringing upon citizens privacy, regardless if they are located within the UK or not. The traffic data can tell an investigator that you consulted specific websites, or search for specific key terms for instance. For example, traffic for Internet users located in the US is sometimes routed through the UK, before entering other jurisdictions. When the traffic passes through the UK, US Internet users will face the same consequences than British ones: a potential breach of their privacy, and the potential use of their data by law enforcement to solve cases.

The Joint Committee examining the Draft Communication Data Bill has already heard ample evidence from witnesses to shed doubts on the Bill. This article reviews the argument put forward by the witnesses. It first explains the current legal framework before delving into the changes that the Bill seeks to introduce.

Existing Legislations

Since the Data Retention (EC Directive) Regulation 2009, article 4 compels public communications providers to retain communication data on fixed network telephony, mobile telephony and the Internet. For the latter, this encompasses Internet access details and e-mails. Each transaction made with other websites does not have to be

recorded by the service providers, nor voice over IP exchanges. Part I Chapter II of the Regulation of Investigatory Powers Act 2000 regulates the access to the retained data and the grounds to do so.

Under the Regulation of Investigatory Powers Act, no judge needs to issue a warrant for giving access to the police of communications data. The warrant comes instead from within the executive branch. Three people within the same entity are in charge of authorising the request: a designated person who 'independently' considers the request, the single point of contact who acquires the data who ensure the legality of the request, and the Senior Responsible Officer responsible for the 'overall integrity of the process'.[3] Even for accessing the content of communications, Secretaries of State authorises the interception, avoiding the involvement of the judiciary branch.[4] A judge will only intervene if the data are encrypted. The Interception of Communications Commissioner functions as an oversight entity that reviews all the requests after the designated person and the single point of contact have granted them to the police authority. The police also report errors to the Commissioner, which numbered 895 in 2011, mainly due to public authorities asking for the incorrect time period or the incorrect type of data.[5] There are few mistakes, and their impact for the users may be limited as the affected individuals are not aware of the breach.

David Davis' answer to the Joint Committee, when asked if he had any evidence of individuals who 'suffered harm as a result of their communications data being accessed by an investigator', is telling: 'not in a critical area, but if you had asked us that question about phone hacking by newspapers five years ago, the answer would have been the same'.[6] The harms suffered by the victim can only appear years later, if it ever appears. The Commissioner has to review all the requests with a limited team of seven individuals, implying that many more breaches may also remain undetected. Justice, a privacy advocate organisation, also criticises 'the oversight work of the Interception Commissioner [for lacking] sufficient transparency'.[7] Michael Ellis, a British member of parliament, strongly suggests that it would not be feasible to have an independent organization approving all requests regarding their sheer number.[8] As noted by the privacy expert Daniel Solove, the executive branch of power, which include authorities taking the decision for accessing communications data, often overweigh security over privacy.[9] For this reason in particular, the implication of the judiciary (e.g. a judge or a magistrate) can ensure a more appropriate accountability of authorities that attempt to shift the balance between security and privacy. Involving the judiciary upstream of the request rather than later as it is the case when a commission review past authorisation implies preventing the breach to privacy to happen, rather than simply noticing it.

Purpose of the Bill

Under the current regime, the Home Office contends that the police have now only access to 75% of all necessary communications data, where it used to be 100% when only fixed and mobile telephony existed.[10] It acknowledges it is impossible to have now full access to all communications data, but hopes that with by forcing all communication service providers (which include Internet service providers) to record all communications data, it will reduce the gap from 25% to 15%. Is a ten-percentage point increase in access of communications data worth sacrificing users' privacy? Does the police really need these data to solve cases? Would the law really lessen the users' privacy? How can we ensure a proportional application of the law? Should it be proportional and exclude the use of communication data for non-serious crime, such as speeding tickets?

In 2011, under RIPA Part I Chapter II, the police filed less than 500,000 requests to access communication data, of which the largest party concerned subscriber data.[11] Subscriber data consists only of matching a number or an IP with address with the person's identity. It constitutes in other words a reverse look up, which is not as privacy invasive as requesting traffic data. Traffic data includes the routing, time and duration of a communication, and include who an individual has sent e-mails to for instance. This type of request represented only a quarter of all requests.[12] The high number of half a million requests is not representative of the number of people it concerns, as the police can request between ten and forty data just on one suspected criminal.

An overseeing authority, such as the Interception Commissioner, despite all the fallacy associated with it, is essential to ensure that the police do not use the law to watch citizens in a disproportionate manner. For instance, in 2008, the local Poole Borough Council used the power in Regulation of Investigatory Powers Act 2000 to watch a family suspected of sending their children outside the school catchment zone. Part I Chapter II of the Act specifies that the

followings justify access to communication data: national security, preventing or detecting crime or preventing disorder, interests of the economic well-being of the United Kingdom, public safety, protecting public health, assessing taxes, preventing death or injury. The range of application is very broad, and the Council putatively claimed that it was in order to preserve the interest of the United Kingdom. The family, outraged, explained that the council did not even come to ask for utility bills to prove their address.[13] The council used disproportionate means for such a situation. What made the use of surveillance disproportionate? The psychological harm caused to the family is somewhat limited to their trust in the council being undermined, especially as the police could have used other means that would not have intruded into the family's private sphere. On top of the harm, the extent of the threat did not justify the use of such intrusive means. An appropriate breach of privacy for security purposes is conceivable in cases when the cost (be it human or economic) of not breaching privacy outweighs the risk of the threat. Sending schools to the wrong school hardly constitute a threat for society. In fact, the article 8 of the European Convention on Human Rights foresaw cases where the state can breach privacy. These cases are: national security, public safety or the economic well being of the country, the prevention of disorder or crime, the protection of health or morals, and the protection of the rights and freedoms of others. Sending children outside the school catchment zone is therefore not included.

The same arguments are valid for the Draft Communication Bill. In their hearing by the Joint Committee, all members of law enforcement agencies converged in saying that they needed more resources for their investigation.[14] As stated previously, the executive favours security over privacy and makes the case that it is legitimate to reduce lessen the privacy of millions of individual for the greater good of society. But they did not explain if they could still carry out their investigation using other tools, somewhat less pervasive. It is very difficult to know the role of data communications in their operations and if they could have used other investigation means. Currently, most of the data communication requests concern drugs related offenses and property offenses.[15] These are serious enough crime to declare the use of communication data as proportionate. Yet, empirical evidence from another European country, Czech Republic, rather suggests that solving crime is not conditional on accessing communication data. In 2011, the constitutional court of Czech Republic declared unconstitutional the data retention law transposing the European Union directive 2006/24/EC. Subsequently, the police could not use communications data as it used to. But what could have caused a hindrance to solve case did not show up in the statistics. The clearance rate increased from 37.55% to 38.54% between 2010 and 2011.[16] The more information the police obtain, the more it has to wade through it and the more difficult and complex it can become. The evidence that these statistics are replicable throughout years and different countries is scant, but policy makers and legislators should keep it in mind. By augmenting tremendously the number of data available to them, the increase in complexity also imply that it makes it more difficult to find the relevant information, if it is even there. Wading through traffic data, a police officer could genuinely mistake a user's behaviour for suspicious when it does not in fact pose any threat. Imagine for instance a person consulting a lot of material on bomb makers because the individual is a writer and needs it. The police officer by spending time in clearing the individual decreases its efficiency (as well as the individual's privacy at the same time). Hence, the access to 10-percentage point higher of data is not guaranteed to increase clearing rates by a significant amount. Would mistakes constitute the rule rather than the norm under the new Bill? By increasing data, one increases the likeliness of police officers to commit mistakes, and the likeliness that unauthorised individuals will access the data.

Conclusion

Proponents to the Bill fear that collecting more data will either not help the police, or that they could find other means to solve crimes. The lack of oversight for such important data collection could lead to many abuses for people not only located in the UK but worldwide. It increases the likeliness of breaches of personal data occurring either inadvertently or as a result of a malicious attack on the information systems of the service providers. It is not clear that the 10% gap that the Home Office is trying to fill by accessing all communications data exists. It is also not clear that the Bill will yield the intended results. But it is sure to cause important privacy disruptions and may even push users to hide further their communications data. Instead of helping law enforcement agencies, the Bill can encourage users to encrypt their data, which can in turn just make the work of the police a lot more difficult.

—

Clement Guitton *is a PhD candidate in War Studies at King's College London. He previously worked at the International Telecommunication Union, a United Nations specialised agency, and holds two masters, one in international relations and one in electrical engineering.*

[1] *United Stated of America v. Jeffrey Lee Parson*,(2003).

[2] Sophos, "Blaster-B worm author sentenced to 18 months in jail – but bigger villain remains free, Sophos reports," *Sophos*, 28 January 2005.

[3] Paul Kennedy, "2011 Annual Report of the Interception of Communications Commissioner," (London: Interception of Communications Commissioner, 2012), p.27.

[4] Home Office, "Interception of Communications : Code of Practice," (London: Home Office, 2002), p.7.

[5] Kennedy, "2011 Annual Report of the Interception of Communications Commissioner," p.30.

[6] Joint Committee on the Draft Communication Data Bill *Draft Communication Data Bill (11 July)*, 11 July 2012, p.8.

[7] Metcalfe, "Freedom from Suspicion : Surveillance Reform for a Digital Age," p.55.

[8] Joint Committee on the Draft Communication Data Bill *Draft Communication Data Bill (17 July)*, 17 July 2012, p.4.

[9] Solove, *Nothing to Hide : The False Tradeoff between Privacy and Security*: p.40.

[10] *Draft Communication Data Bill (10 July)*, p.3.

[11] Kennedy, "2011 Annual Report of the Interception of Communications Commissioner," p.29.

[12] Ibid.

[13] BBC News, "Council admits spying on family," *BBC News*, 10 April 2008.

[14] Joint Committee on the Draft Communication Data Bill *Draft Communication Data Bill (12 July)*, 12 July 2012.

[15] *Draft Communication Data Bill (10 July)*, p.5.

[16] UN Watched, "Tschechien: Neuer Anlauf zur Wiedereinführung der Vorratsdatenspeicherung," UN Watched, https://www.unwatched.org/EDRigram_10.11_Tschechien_Neuer_Anlauf_zur_Wiedereinfuehrung_der_Vorratsdatenspeicherung?pk_campaign=edri&pk_kwd=20120606.

About the author:

Clement Guitton is a PhD candidate in War Studies at King's College London. He previously worked at the International Telecommunication Union, a United Nations specialised agency, and holds two masters, one in international relations and one in electrical engineering.