INTRODUCTION

The controversial PRISM programme has uncovered a global reality of trans-border law enforcement access to private sector data, triggered by cloud computing. Law enforcement agencies (LEAs) are indeed increasingly targeting foreign cloud computing service providers and, as put by Europol, cloud computing “will continue to have a profound impact on law enforcement investigations.” This reality poses challenges to both state interests and individual rights, as it does not only disturb the relations between sovereign states, but also causes legal uncertainty for the individual as regards the applicable privacy and data protection standards for law enforcement access to personal data and metadata in the fight against cybercrime. The distinction between personal data and metadata becomes irrelevant when cross-referencing several sources of data about one individual. Moreover, metadata might be even more revealing than content, so that it can be said that big data “exacerbate the existing asymmetry of power between the state and the people.”

CHALLENGES TO SOVEREIGNTY

Technology allows state officials to gather evidence and take actions outside their territorial scope without permission from other states. Law can and does acknowledge this either by extending the scope of existing powers or by creating new powers with an explicit extraterritorial reach. In that regard, two Belgian investigative measures

---

1 Paul de Hert is Professor at the Vrije Universiteit Brussel (Belgium) and the Tilburg University (The Netherlands). Gertjan Boulet is a Doctoral Researcher at the Research Group on Law, Science, Technology and Society (LSTS) at the Vrije Universiteit Brussel.


are emblematic for a global reality where sovereignty is affected by the trans-border reach of national investigative powers. First, the Belgian Supreme Court held that Article 46bis of the Belgian Code of Criminal Procedure (CCP) can also be applied to a foreign provider of electronic communications services (Yahoo!) to hand over identification data.\(^8\) Secondly, the Belgian lawmaker created the power of the network search (Article 88ter CCP) allowing an investigative judge,\(^9\) when performing a search on a computer system, to extend this search to another computer system even outside the Belgian borders and without formal request for mutual legal assistance. The extraterritorial reach of this network search has been justified by considerations of time and risk of evidence loss in cases of serious crime, but backed by principles of necessity, proportionality and a posteriori notification.\(^10\)

The Belgian Yahoo case and the network search powers raise questions about the scope of territorial jurisdiction, respectively the legality of international hacking and extraterritorial jurisdiction in cyberspace. In that respect, Hildebrandt rightly posits that “[t]he fact that the Internet facilitates remote control across national borders at low costs basically means that the fundamental assumptions of territorial criminal jurisdiction will increasingly fail to describe accurately what is a stake”.\(^11\)

Considering the lack of any effective international initiatives for trans-border investigations on the Internet, it would be unrealistic to prohibit national extraterritorial initiatives for trans-border access.\(^12\) Moreover, current discussions on the international level even seem to endorse such practices.

First, at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, an International Group of Experts prepared an unofficial (draft) “Tallinn Manual on the International Law Applicable to Cyber Warfare”.\(^13\) The Manual provides that without prejudice to applicable international obligations, a State may exercise its jurisdiction extraterritorially, in accordance with international law. The Manual further recognizes the impact of cloud computing on jurisdiction, but provides that “[a] State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.”\(^14\) This raises questions about the legality of international hacking, and the role of a posteriori notification duties.

Secondly, the Cybercrime Convention Committee (T-CY) of the Council of Europe has been discussing the development of an Additional Protocol to the Cybercrime

\(^9\) An investigative judge is a magistrate charged with the task of gathering evidence in a case. Investigative judges only exist in the inquisitorial system used throughout continental Europe.
\(^14\) Ibid., pp. 27, 33.
Convention on trans-border access. In a discussion paper of December 6, 2012, the T-CY put that “the Belgian solution offers great opportunities to handle data stored in ‘the cloud’. [...] [and] makes clear that it is not important to know where the data is stored, but from where it is accessible.” This could mean that the T-CY considers the Belgian network search as an exceptional circumstance under which it would allow hacking. In a guidance note of February 19th, 2013, the T-CY underlined that Parties “may need to evaluate themselves the legitimacy of a search or other type of [trans-border] access in the light of domestic law, relevant international law principles or considerations of international relations.” In the recent draft elements for an Additional Protocol of April 9th, 2013, the T-CY recalled to avoid international hacking, but at the same time proposed far-reaching options for trans-border access.

Model provisions on notification duties can be found in the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union which contains a section on the “Interception of telecommunications without the technical assistance of another Member State” (MS). The intercepting MS shall inform the notified MS of the interception prior or after the interception depending on whether it knows when ordering or becomes aware after the interception that the subject of the interception is on the territory of the notified MS. Until the notified MS decides if the interception can be carried out or continued, the intercepting MS may continue the interception and use the material already intercepted for taking urgent measures to prevent an immediate and serious threat to public security.

In these documents we see a first set of good ideas about regulating trans-border law enforcement. ‘It can be done’ and ‘it has advantages’, the documents seem to suggest, but sovereignty needs to be protected as much as possible, through creating some sort of transparency before or after interventions by the law enforcing state.

We now turn to the challenges that trans-border law enforcement access to private sector data poses to the rights to privacy and data protection.

---

16 Ibid., pp. 50, 57.
Challenges to the rights to privacy and data protection

A cybercrime report of the United Nations Office on Drugs and Crime contains a section on “extra-territorial evidence from clouds and service providers”, which provides that the Cybercrime Convention does not adequately cover situations of trans-border access due to provisions on consent of the person with lawful authority to disclose the data. In its draft elements of April 2013, the T-CY also moved away from a strict condition of consent, but which evoked criticism from academics, private sector and civil society. Considering the apparent lack of trust in the transparency and accountability of governments, it can be said that complementary private sector instruments addressing their own transparency and accountability in law enforcement, would give the individual at least some parts of the puzzle on his or her fundamental rights status on the table. For instance, Google and Microsoft are increasingly providing transparency about their cooperation with LEAs. Moreover, Microsoft hosted a series of five privacy dialogues to discuss “the role of individual control and notice and consent in data protection today, as well as alternative models that might better protect both information privacy and valuable data flows in the emerging world of Big Data and cloud computing.” The final Global Privacy Summit yielded a report underpinned by a respect for information privacy principles.

Conclusion

The global reality of trans-border law enforcement access to private sector data, triggered by cloud computing, undermines both state interests and the rights to privacy and data protection. Challenges to sovereignty relate to the scope of territorial jurisdiction, and to the legality of international hacking and extraterritorial jurisdiction in cyberspace. Challenges to the rights to privacy and data protection relate to the existing legal uncertainty for the individual as regards the application of privacy and data protection standards, including the role of individual consent, for law enforcement access to personal data and metadata in the fight against cybercrime. Current international documents seem to suggest full protection of sovereignty, through a priori or a posteriori notification duties for the law enforcing state. Yet, considering the apparent lack of trust in the transparency and accountability of governments, complementary private sector instruments addressing their own transparency and accountability in law enforcement could arguably give the individual at least some parts of the puzzle on his or her fundamental rights status on

the table. Although the challenges at stake still need to be addressed in the greatest
detail, current documents can and should already be critically assessed in that respect.