FACULTY OF LAW, UNIVERSITY OF AMSTERDAM
Institute for Information Law

Dr. Kristina Irion, LL.M.
Vendelstraat 7
1012 XX Amsterdam
The Netherlands
Tel: +31-20-5253406
E-mail: k.irion@uva.nl

Amsterdam, 6 April 2016

"The Reform of the e-Privacy Directive: How to get it right?", Public conference organized by the Greens/ EFA, 6 April 2016, European Parliament, Brussels

The forthcoming review of the Directive 2002/58/EC (as amended, e-Privacy Directive) will impact on the future of confidentiality of communications. My comments address some of the challenges and issues that have to be addressed in order to get it right.

1. Confidentiality of communications

Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention on Human Rights (ECHR), and the constitutions of member states (Recital 3 of the e-Privacy Directive). In constitutional law, in order to give effect to a human right in the private sector, it is necessary to pass legislation. In the current e-Privacy Directive confidentiality of communications is guaranteed in Article 5(1) and covers the content of communications and related traffic data.

In relation to the new GDPR

Confidentiality of communications is not compensated with the enactment of the new General Data Protection Regulation (GDPR). A duty of confidentiality requires qualitatively more protection than what general EU data protection legislation affords. The legal institute necessitates that users have a right to confidentiality of qualified communications and a corresponding duty to confidentiality on part of the providers. In order to give effect to confidentiality of communications, the review of the e-Privacy Directive should accomplish to better entrench user's right and providers' duty.

Scope of application

The scope of application of the e-Privacy Directive is outdated by technological developments as well as the international and distributed supply of communications services. As a result, the scope of application of confidentiality of communications became increasingly limited to telecommunications services in the traditional sense. Under the present regime, a host of new communications services are not covered by confidentiality of communications and, above all, its protection is no longer end-to-end.

For example:
- certain over-the-top (OTT) services and embedded communications (e.g. messaging inside dating apps);
- closed user groups and private community functions (e.g. social network sites, publicly available VPN services);
- device manufacturers and certain intermediaries are not bound by confidentiality duties; and
- mobile devices with embedded SIM-cards (tablets and e-readers).

In order to preserves its essence, a functional approach to the scope of application would be advisable, with respect to confidentiality of communications. A future concept of confidentiality of communications should cover in a technologically neutral fashion:

i. any private communications between a finite number of parties;
ii. from end-to-end; and
iii. that are made available to EU citizens and legal persons (even if the services are supplied from outside the EU).

Substantive scope

The substantive scope of confidentiality of communications today covers communications and traffic data. Communications already includes any information transmitted by an infinite number of users, hence voice, image and data conveyed. It is unclear whether confidentiality of communications would extend to individual transactions with services providers and automated interfaces, such as cloud services. There is also a clarification necessary, that automated scanning of communications (e.g. Gmail practice) is in conflict with the confidentiality of communications if it is done without the consent of the users.

Traffic data is also broadly defined and covers any data processed in the conveyance of communications. The review should clarify that traffic data also comprises of the location data and, hence, location information would be protected by confidentiality of communications.

Individual's consent

Outside of the purposes provided for under the law (e.g. technical conveyance, law enforcement, fraud prevention), providers can process individuals' communications and traffic data on the basis of users' explicit consent. In order to contain the excessive reliance on individual's consent, it would be necessary to unbundle the communications service and individuals' consent to any service features from using communications and traffic data for other purposes than providing the service (e.g. targeted advertisement, profiling, transfer to third parties, etc.).

2. EU law and national data retention measures

The e-Privacy Directive explicitly applies to member states' national data retention legislation. Art. 15 (1) allows Member States to adopt data retention measures for a limited period only "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security...". This provision has two purposes: First, it clarifies that national data retention measures are within the scope of EU law, and, second, it set's out some qualified requirements for the adoption of such measures. Abolishing this reference does not necessarily mean that the CJEU would not apply EU law and, hence, the Charter to national data retention legislation. However, the link would be much less straightforward.