# PRIVACY VS. SECURITY? A DILEMMA OF THE DIGITAL ERA

Over the coming years a crucial issue in dealing with cybercrime will be the delicate balance that must necessarily be struck between personal data protection, public order, and security.

If the stellar growth in e-commerce in the last decade, was accompanied by increasing alarm about the attendant potential for fraud (from e-bay scams to credit-card cloning), the next ten years seem bound to be beset by the headaches of cloud computing: who knows what dormant dangers may be inadvertently aroused merely by surfing the web, even without posting personal data online, or using social networks (all of which are exposed to data mining)? In this specific context, given the enormous wealth and value of the information that can be gleaned from the hard drives of individual PCs, from mere web searches, not to mention electronic intercepts, digital forensics and cloud computing which will certainly play an ever more decisive role in criminal investigations. This trend, already underway, was recently most singularly highlighted in the capture of a fugitive member of the "N'drangheta" (a Mafia-type organization operating in Calabria), one of Italy's 100 most-wanted criminals, arrested because he frequently logged on to his personal Facebook account using the nickname "scarface."

Social networks and digital data in the public domain

Digital data useful for law-enforcement purposes, may be broadly divided into information identifying a suspect (IP Address), data retracing the latter's web-browsing history (server logs) and the content of the suspect's online correspondence (electronic intercepts). This type of data is indispensable for identifying a person in the course of digital investigations. Although this kind of information is accessible, as a general rule, only on the basis of warrants, subpoenas or other discovery orders issued by the relevant authorities against Internet service providers, a great deal of the data in question may, in fact, be obtained indirectly through simple web searches.

Corporations such as Intelius Inc., offer an impressive array of highly effective services, supplying, for a fee ranging from $1 to $10, information on each and every US citizen, including residential address, fixed-line and cell phone numbers, e-mail address, criminal records, creditworthiness, employment history and level of education.
Date Check, one of Intelius' cell-phone supported services, for instance, provides users with a full profile of potential dates, with nothing more to start with than their telephone number. The information offered includes not only personal data, but also the target's criminal record, if any, as well as his or her earnings and assets, academic qualifications, and most crucially, current marital status, all delivered in a matter of seconds and a few clicks on users' mobile handsets, so as to help them decide whether to start or continue a romantic relationship.

Intelius Inc. states on its website that all the information it provides is gleaned from public records: if true, this means that public data placed online on a daily basis, holds the keys to a vast variety of significant information which, until very recently, was considered beyond the reach of prying eyes.
The user profiles on Facebook or any other social network can be mined not only to reveal the account holder's identity, but also to "intercept" all the chats, posts and data passing through the account, so as to analyze their content for information useful to law enforcement agencies.
It is, therefore, obvious that data must also be classified on the basis of whether or not they are accessible to the public. The need for such a distinction is all the more pressing given that, so far, it has received scant consideration at European level.
The U.S. Supreme Court has held that "the Fourth Amendment does not prohibit "the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose." If these principles are to be applied unmitigated in their present form to the emergent reality of Web 2.0, they would enable intelligence and law-enforcement agencies to indiscriminately mine all information posted on social networks.

According to the results of a survey of over 2,000 Canadian undergraduates by Toronto-based Ryerson University's Privacy and Cybercrime Institute, young people overwhelmingly tend to believe that information shared over personal networks was automatically protected by a sort of "network privacy" that did not however extend to content posted on websites. In sharp contrast with this view, the same study found, businesses and academic institutions recognize no such notion and consider all information posted online, fully in the public domain and undeserving of protection.
As the online information that could prove useful for solving, fighting and thwarting crime continues to grow in both quality and quantity at a breathtaking pace, law-enforcement agencies are bound to increase their reliance on data-mining techniques. It is therefore urgent that at least the courts focus greater attention on the type and manner of acquisition of online data deemed admissible as evidence in criminal trails.
Lastly, as European data protection agencies have repeatedly pointed out, it is also important for users, both young and not-so-young, to take greater responsibility for the type of content they post on these "virtual private premises."

Data retention and Digital wiretapping: US and Europe have adopted two different approaches

Besides playing a crucial role in digital investigation, IP addresses can also be used to profile users for commercial purposes, especially in combination with cookies, as underscored in the recent European e-privacy Directive (2009/136/EC).
In 2008, the German data protection commissioner, Peter Schaar, who headed the Article 29 Data Protection Working Party (comprising all European privacy authorities), expressed the view that IP addresses constitute personal data, and as such, are protected under the European e-privacy Directive. His remarks sparked a lively debate with certain US corporations which argued, on the contrary, that since an IP address did not, in itself, identify the user, so it could not be deemed personal information meritorious of protection under privacy regulations.
Torn between demands from European data protection authorities and US privacy rights groups to curtail data retention on the grounds that corporations like Microsoft, Google and Yahoo currently store far too much identification data for far too long, on the one hand, and calls by law-enforcement agencies for even

more data be stored for ever longer periods of time, on the other, ISPs are at a loss to decide which direction to take.
Although Europe has opted for highly detailed data retention regulations (Directive 2006/24/EC, Article 5 states that IP addresses and server logs may not be stored for less than six months or more than two years), the issue is by no means settled. Calls for similar regulations in the U.S. were met with vigorous opposition and loud protests by both the EPIC (Electronic Privacy Information Center) and the EFF (Electronic Frontier Foundation).
There was no dearth of criticism in Europe either: Article 29 of the Working Party's document entitled "The Future of Privacy" noted that the Directive not only lacked some adequate and specific safeguards as to the treatment of communication data, including provisions requiring an indication of the purposes for which the data are stored, or of the persons and parties authorized to access the retained information, but also failed to clarify the types of data that may in no event be lawfully stored or retained by ISPs and connectivity providers.
Recently, the German Constitutional Court outlawing the national legislation on mass storage of telephone and web traffic data, passed in implementation of the Directive. The practical repercussions of this scenario are clear: when dealing with an ISP in a jurisdiction bereft of data retention regulations, such as the U.S., or Germany, law-enforcement officers could never be sure if the information they seek has long been cancelled or is still in storage and admissible as evidence.
Electronic interceptions of online communications are even greater cause for concern in terms of privacy protection, than merely identifying a user and perusing his/her web-browsing history. Unlike phone calls, e-mails can be immediately indexed using specific tags, and often contain exceedingly useful attachments as well as other information shedding light on the context of the exchange.
The fact that electronic intercepts make it possible to glean information which is undeniably more useful than that obtained from telephone wiretaps does not seem to foster forms of transnational cooperation that are more effective than the bilateral instruments on mutual legal assistance currently in force. This issue is particularly delicate since the world's largest "holders" of digital information are US-based corporations.
In a comment made at the 2001 Cybercrime Convention (which was also ratified by the United States), the Council of Europe laconically presented the issue of a Party permitted to unilaterally access computer data stored in another Party without seeking mutual assistance, stating that such a case is particularly complex and could not be resolved "in part (...) due to a lack of concrete experience with such situations to date."

Conclusions

While this article is intended to highlight the differences between the European and US approaches to privacy rights and public order and security, and to spark further research and debate on the issues involved, it does however lead to three preliminary conclusions.
First and foremost, there are no winners or losers in the efforts to strike a balance between personal rights and public order and security, as these two following examples illustrate. On the one side, Europe adopted a data retention policy necessitating clearer definitions of the types of offences in connection to which stored personal data may be subjected to disclosure. On the other side, during the Bush administration the National Security Agency struck a deal with the main national telecommunications carriers to set up a database of the records of all the phone calls and online activities of American citizens.

Secondly, the EU-US joint statement released in Washington on 28 October 2009, as well as the Stockholm Program of 2 December 2009, are and must be treated as urgent calls for the active implementation of the Cybercrime Convention. Without wishing to belittle the importance of this Convention, however, it is clear that in an area such as Internet which connects the entire world, Intergovernmental Organisations also need to intervene, endeavouring to include as many countries as possible.

The third and last conclusion is more of a hope: the huge potential of the Internet cannot be exploited merely to keep in touch with old classmates or make free video calls to family and friends. It is precisely as a result of the global interconnectivity it offers, allowing people from different countries and backgrounds to share information and exchange ideas, that the Internet must serve as the starting point for setting up a framework of rules that reconciles privacy protection with the public interest in detecting, investigating and preventing crime both online and offline, in a manner satisfactory to all. We managed to draw up the Universal

Declaration of Human Rights without the benefit of the Internet as a universal instrument of peace. Imagine what we can now do, with it.

* Giuseppe Vaciago is a lecturer in IT Law at University of Milan, focusing his research on cybercrime and computer forensics.