CNIL Newsletter on Innovation and Foresight

N°03 / July 2012

IP INNOVATION & PROSPECTIVE

Follow us on the website [www.cnil.fr/ip] by scanning the QR Code or on

IP - EVENT

The first Privacy Camp in Europe

The digital community and CNIL come together to share views on personal data control online.

Panorama of privacy protection tools

More and more 'privacy protection' tools are becoming available for the general public, but what are the aims of those developing and promoting them? A general survey.

Three questions to Jean-Marc Manach

OWNI journalist and Le Monde blogger (Bug Brother) Jean-Marc Manach is a specialist on digital liberties and issues relating to surveillance and privacy protection. He is the author of *"La vie privée, un problème de vieux cons ?"* and *"Au pays de Candy : enquête sur les marchands d'armes de surveillance numérique"*.

IP - FOCUS

Service robots – at the center of future ethical and legal debate?

A report submitted to the Ministry of Industry considers the future of service robots in France. Assisting the elderly or disabled, companions or domestic robots, security and surveillance – these are the most likely emerging markets. However, ethical and legal issues remain unclear, and "privacy" will be the focus of increasing attention as these robots become part of our daily lives.

According to Symantec, the cost of data breach incidents for French companies is constantly rising

The Symantec study published in March 2012 on the cost of data breaches reveals that the cost has risen by 16% to reach an average cost per compromised record of €122.

News in brief...

Key figures.

How can we control our personal data online?

At a time when personal data has become a highly marketable commodity, finding an answer to this question is no simple task. Even so, no one can question the need for tools that will allow Internet users to regain control of their data and help build up trust in the digital economy.

Last March, CNIL organized its first Privacy Camp on just this issue, with participants attempting to answer this difficult but crucial question.

For CNIL, the event was a real innovation in terms of both form and content. Jointly coordinated by the Department of Studies, Innovation and Foresight and the Communication Department, its success proves that CNIL is on the right track with its open, collaborative approach.

The Privacy Camp provided a forum for enthusiastic debate as well as criticism. A number of novel and imaginative proposals emerged, including some put forward by CNIL's innovation laboratory. Discussions focused on tools, practices, and services aimed at helping users learn more about online personal data flows and 'leaks' and control privacy online.

The event was also an opportunity for CNIL to embark on an initiative based on sharing and collaboration that is part of its plan to develop an open approach to innovation, in favor of privacy and personal data control. Other events and initiatives are planned.

Sophie VULLIET-TAVERNIER,
Head of Studies, Innovation and Foresight ■

Europe's first Privacy Camp: the digital community gathers to share views on personal data control online

On March 30, 2012, the digital community took over La Cantine (see box), for a half-day event initiated by CNIL to address the issue of "how to control personal data online".
The event was organized as a BarCamp or "unconference", open to anyone wishing to attend its participant-driven workshops. The agenda is created by attendees, who must all contribute, in one way or another, based on the "no spectators, only participants" principle.
Jointly organized by CNIL, Mozilla, Owni and Silicon Sentier, the event was a great success, drawing a hundred or so attendees from a wide range of backgrounds (ordinary Internet users, experts, developers, journalists specializing in the digital world, researchers and academics, students, digital liberties activists, designers, and business people) to talk about tools, practices, and services designed to help control privacy online, and learn more about online personal data flows and 'leaks'. CNIL's Expertise Department presented a tool designed by the CNIL Innovation Laboratory for real-time visual representation of cookies.
A videoconference on data protection in America was organized with Shaun Dakin, the promoter of PrivacyCamps in the United States[1]. PrivacyCamps were organized in Washington and San Francisco in 2010 and 2011 to coincide with the Privacy Identity Innovation conference. Another such event was held in Canada in June 2010, supported by the Office of the Privacy Commissioner of Canada. Shaun Dakin mentioned in particular the ongoing debates on the White House's "Consumer Privacy Bill of Rights"[2].

Participants proposed and led 11 workshops on the following topics:

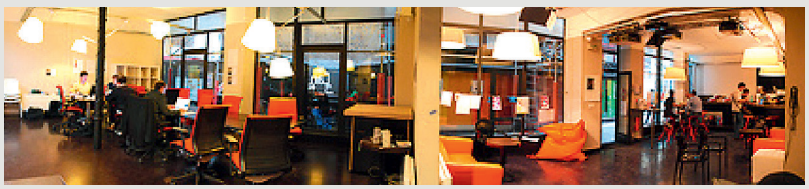
1. Anonymous or not?
2. Distributed or decentralized social networks.
3. Cell phones and privacy.
4. All our personal data exposed online: why we can't control our data once it's online (demo).
5. Free economic models versus Privacy.
6. Tracking tools: cookies, chip card readers (demo).
7. The WebID concept.
8. Online awareness and reputation.
9. Anonymity tools (demo).
10. Is it possible to manage several identities?
11. Hack the CNIL? How to go on from there...

The workshops addressed a very wide range of topics, asking questions such as what Facebook will be like twenty years from now after a long period of data accumulation. Two workshops looked into the concepts of decentralized social networks and the technical solutions needed for their large-scale use, such as the WebID protocol, a universal standard for identity and login that is being developed by a W3C group[3].
Participants also explored anonymity and pseudonymity in their various forms, as well as the tools designed to preserve them. For example, although the free software and open network TOR enables browsing to be anonymous, it can also make it slower. As with encryption, tools must be adapted to meet real requirements without starting an 'arms race'. Another workshop attempted to clarify the directly related issue of managing several identities, considering how it could be achieved and why it was useful. Identity segmentation springs from a desire to adapt to different contexts but can be difficult to achieve in technical and practical terms. It can even have the opposite effect to that intended.
A long debate ensued on educational aspects and the need for concrete demonstration tools to make people more aware of tracking. Efforts in this area should not stop at heightening risk awareness, however, but also offer concrete solutions, taking care to avoid messages that serve no purpose other than to increase anxiety. In this respect, CNIL should not only show how we are tracked, but also how we can protect ourselves and choose the right level of protection.

For CNIL, the event was a pool of new ideas, confirming the advantages of the open approach to innovation it wishes to promote. A collaborative report (available on cnil.fr/ip) testifies to the quality of the discussions. Many different opinions were expressed on currently available tools, their advantages and their ease of use. Participants also discussed what tools they would like to have available in the future.

Anne-Sophie Jacquot
Geoffrey Delcroix ■

La Cantine : a coworking venue for everyone in the digital community



La Cantine, located in the Passage des Panoramas in Paris, is run by Silicon Sentier, an association that brings together 170 start-ups and SMEs. It is a place where people can work – it is the first coworking space in Paris – and organize events for the digital community. La Cantine sees itself as a place where "programmers, developers, technology enthusiasts, innovators, business people and users can meet and exchange views".
http://lacantine.org/

1. http://twitter.com/privacycamp
2. http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
3. http://www.w3.org/wiki/WebID
4. https://www.torproject.org/

Three questions to... Jean-Marc Manach

OWNI journalist and Le Monde blogger (Bug Brother) Jean-Marc Manach is a specialist on digital liberties and issues relating to surveillance and privacy protection. He is the author of "La vie privée, un problème de vieux cons?" *and* "Au pays de Candy: enquête sur les marchands d'armes de surveillance numérique".

Do you think we can still protect our personal data online or is the battle over before it has begun?

Following the Google portrait of an 'anonymous' Internet user, published by the magazine *Le Tigre* and based on photos, videos and information that the user had shared on the web and social networks, a journalist decided to draw 'my' Google portrait[6]. Although I have been an active Internet user, journalist and defender of liberties and privacy for more than ten years, he didn't find any 'sensitive' information about me, which goes to show that it's quite possible for us to 'protect' our data once we have understood that the Web is a public space, and that any information we 'share' is no longer 'private'. On the contrary, the concept of 100% security does not exist in physical space any more than it does on the Internet, and that is true whether we consider our computers (and therefore our private correspondence, identifiers and passwords) or the personal data that e-commerce and administrative websites demand that we give them. Which explains the importance of notions such as data minimization (keeping shared data to a minimum), privacy by design (i.e. designing privacy protection into services and applications) and, of course, observing the law. As it happens, very few websites have been sued, let alone sanctioned, for having failed to provide adequate protection for their users' personal data.

What can be done to incite people to take greater care of their personal data, without resorting to complex, technical explanations or generating unnecessary anxiety?

We need to trust users and treat them like intelligent, responsible beings. We need to stop being afraid of them and stop frightening them. Messages relating to computer security and online privacy are usually put over in ways that generate anxiety. Unfortunately, the tendency is to make Internet users feel guilty and explain to them that the Internet is complicated and fraught with danger. That is both condescending and counterproductive. There's nothing intrinsically wrong in using the Internet to run our private lives, in fact it can teach us how to lead a public life. And that is what the future of the Internet is all about: we are all becoming public figures. In my opinion, that's a good thing for democracy. The sexual revolution allowed us to contemplate (and teach) sexuality in ways other than just in terms of reproduction and sexually transmitted diseases. Similarly, the development of the Internet should help us understand (and therefore teach) freedom of expression as a supplement to democracy.

What do you say when someone asks for your advice on personal data control?

We need to be clear about one thing: we can no more make our computers 100% secure than we can make our homes 100% secure from burglars. Which doesn't mean we can't take some precautions. American researcher Danah Boyd[7] has frequently explained that young Internet users are better at managing their private lives online than their parents are. Paradoxically, the best way to protect our personal data is to express ourselves, which means having a public life online. Because the more we use the Internet, the more we learn about how to master its uses, services and tools and thus to control machines. Letting the machine control us and dictate to us what we can and cannot do means giving someone else responsibility for protecting our data. And we can only protect what we can control[8].

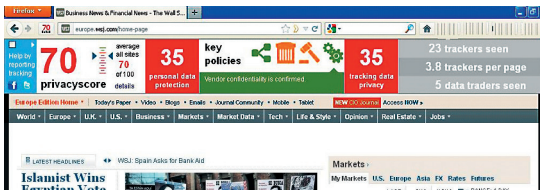
Ever more tools for privacy protection and control

Recent months have seen the arrival of a growing number of tools aimed at helping Internet users understand more about the tracks they leave behind them on the Web and how they are followed. These tools, which are often very well designed and practical to use, could at last appeal to a wider audience, and not just to geeks who either use more complex encryption and anonymity tools, or solutions that call for long parameter settings or advanced technical knowledge.

Most new tools in this area are used with very widespread products, usually as web browser add-ons. One of the most famous is called Collusion[5], an add-on for Firefox developed by Mozilla that allows users to see all the cookies and trackers encountered during a browsing session. Mozilla is a non-profit organization, but several private companies have also entered the personal data protection market. Two such examples are Abine and Evidon, which have developed their own tracker blocking tools, respectively "Do Not Track +" and "Ghostery". PrivacyChoice has adopted a different approach. Using its own criteria, it assigns sites a score out of 100 according to their privacy policy and the presence of trackers. This assessment is accessible via a browser add-on (see illustration below). While the approaches adopted by these companies would seem to have their advantages, the assessment criteria they use imply subjective choices that may be related to their economic model. And that brings us to what could be the big question tomorrow (setting aside problems of daily use): how far can we trust these economic stakeholders and how do they determine whether a cookie is 'good' or 'bad'?

Free or more specialized tools are also available. CNIL will soon be posting a video tutorial on its website explaining how to limit the tracks we leave on the Internet and taking a look at the AdBlockPlus and ShareMeNote browser extensions and the DuckDuckGo search engine.

Geoffrey Delcroix ■



Example: "PrivacyScore" of the Wall Street Journal website according to PrivacyChoice.

5. http://www.mozilla.org/en-US/collusion/
6. "*Tout ce que vous avez toujours voulu savoir sur moi mais que vous aviez la flemme d'aller chercher sur l'internet...*" http://bugbrother.blog.lemonde.fr/2009/01/16/tout-ce-que-vous-avez-toujours-voulu-savoir-sur-moi-mais-que-vous-aviez-la-flemme-daller-chercher-sur-linternet/
7. "*Vers une vie privée en réseau*" : http://www.internetactu.net/2010/03/18/vers-une-vie-privee-en-reseau/
8. See "*Vie privée: le point de vue des 'petits cons'*" : http://www.internetactu.net/2010/01/04/vie-privee-le-point-de-vue-des-petits-cons/

Service robots - at the center of future ethical and legal debate?

In June 2012, the consultancy firm Erdyn submitted its report on the future industrial development of personal and service robots in France to the Ministry of Industry. The study, available in French on the website of PIPAME[9], an interministerial taskforce on foresight and anticipation of economic change, focuses particularly on three emerging markets for service robot applications: robots for assisting elderly and disabled people, companion or domestic robots, and security and surveillance robots. The study defines the robot as a mechanical device that can perform tasks with independent decision-making capability on all or some of the elementary actions making up the tasks in question. It sets out to assess the strong and weak points of the scientific and industrial fabric and of the French robotics ecosystem at the international level. According to the Erdyn report, legal and ethical issues are often raised in the debate on service robots and their applications (respect for human dignity, privacy, individual liberties, confidentiality, social responsibility, etc.), but seldom resolved. The usual position adopted by market players is that although such ethical questions should be raised, they should not hinder the deployment of robots. In actual fact, it would be better to go a step further and make robots socially, ethically and legally acceptable. But as Ryan Calo points out[10] *"by definition, robots are equipped with the ability to sense, process, and record the world around them."* This means that privacy will be a major issue over the coming years, for if service robots come to be regarded as permanent domestic spies they will no longer be accepted by consumers. If the government comes out strongly in favor of developing service robotics in France, as the authors of the Erdyn report hope, then the ethical and regulatory framework - and privacy in particular - will definitely be one of the keys to large-scale deployment of service robots.

Geoffrey Delcroix ■

9. http://www.industrie.gouv.fr/p3e/etudes-prospectives/robotique/
10. M. Ryan Calo, "Robots and Privacy," in *Robot Ethics : The Ethical and Social Implications of Robotics* (Patrick Lin, George Bekey, and Keith Abney, eds.) Cambridge: MIT Press, décembre 2011.

According to Symantec, the cost of data breach incidents for French companies is constantly rising

A recent survey carried out by the Ponemon Institute for Symantec[11] analyzing data breach incidents at 23 companies from ten different sectors of industry shows that the cost of such incidents to French companies increased for the third year running, rising from Ð2.2 million in 2010 to €2.55 million in 2011. Forty-three percent of personal data breaches are the result of malicious or criminal attacks involving malware, malicious or criminal insiders, theft of data-bearing devices, etc. The cost of such breaches is far higher than that connected with negligence (30% of incidents) or computer system glitches (26%).

The average cost per compromised record rose from €98 to €122. Indirect costs, such as customer loss, account for 57% of this average cost. The total cost related to lost business or contracts amounts to nearly €783,000 for the companies concerned.

The study also shows that French companies were in favor of preventive measures to respond to data breaches: encryption was up 9%, security monitoring system increased by 15%, while terminal security solutions saw a 7% rise.

In the United States, total costs incurred in connection with data loss fell by 24% in a year, amounting to $5.5 million, the first drop observed in seven years. Although the average cost per compromised record dropped by 10% to €146.25 in 2011, it remains higher than in France.

Olivier Coutor ■

Source: "2011 Cost of a Data Breach Study", March 2012
11. http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20120321_01

News in brief...

Two-thirds of British consumers responding to a survey stated that their definition of privacy had changed since the arrival of the Internet and social media, while four-fifths considered that disclosing personal information was increasingly part of modern life. (*Data privacy: What the consumer really thinks 2012*, The UK Direct Marketing Association, June 2012).

300 million photos are published on Facebook every day (First-quarter results 2012, Facebook).

According to a survey by market research company GfK, **3 million** tablets will be sold in France in 2012, a 50% increase on 2011 sales.

In France, 61% of students at junior high school (*collège*) and 49% at senior high (*lycée*) spend **more than one hour a day** posting photos and videos on Facebook. (*"Enfants et Internet, Baromètre 2011 de l'opération nationale de sensibilisation"* Calysto - *La voix de l'enfant*).

Two-thirds of French cell phone users accept the idea of geolocation (the same proportion as in the rest of the world). 31% of them use geolocation-related services (compared with 19% worldwide) and 64% wish to use geolocation services in the future (*Mobile Life 2012* – TNS Sofres, Avril 2012).

In France, **25% of women and 16% of men** admit to spying on their husband's/wife's/partner's telephone, computer, mailbox or Facebook account (Yahoo ! survey, June 2012).

According to a survey by Cisco, the Internet should produce around one zettabyte of data every year as of 2015 (a **zettabyte** is roughly equivalent to 250 billion DVDs).

1.8 billion terabytes of data was created in 2011, of which 90% was unstructured (Cloud and Big Data survey, IDATE, May 2012).

CNIL
Commission Nationale de l'Informatique et des Libertés
Commission Nationale de l'Informatique et des Libertés

Department of Studies, Innovation and Foresight
8, rue Vivienne - CS 30223 - 75083 Paris CEDEX 02
Tel.: +331 53 73 22 22 - **Fax :** +331 53 73 22 00
deip@cnil.fr

Quarterly publication
Publication Director: Yann Padova
Editor in Chief: Sophie Vulliet-Tavernier
Graphic design: EFIL Communication
02 47 47 03 20 - www.efil.fr
Printing: Imprimplus
Photo credits: CNIL, Silicon Sentier, Ophelia Noor - OWNI
ISSN: 2118-9102
Legal registration: Date of publication

www.cnil.fr