IP

INNOVATION & PROSPECTIVE

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

web

STUDIES AND SURVEYS

Survey on "Smartphones and Privacy: Uses and protection measures"

The survey conducted by Médiamétrie on behalf of CNIL provides a status assessment of the practices and perceptions of smartphone users regarding the protection of their personal data.

Three questions to... Stefana Broadbent

A specialist of digital anthropology and behaviors linked to new information and communication technologies, Stefana Broadbent comments the findings of the "Smartphones and Privacy" survey and discusses the impact of smartphones on social links between individuals and their close relations.

FOCUS

How much are your on-line data worth?

A recent Spanish experiment shows that web users are relatively aware of the merchant value of their personal data, but rather opposed to their monetization (Your Browsing Behavior for a Big Mac: Economics of Personal Information Online, 2011).

Assessment on the Web presence of French companies and administrations ?

Several recent studies show that progress is still needed for French companies and administrations.

Exploring issues of privacy via behavior economics

The ANR ESPRI project combines economists, sociologists and lawyers focusing on an analysis of economic behaviors and practices in the field of personal data.

News in brief...

Key figures.

Smartphones and Privacy: towards a new vision of data protection?

In this age of all-digital revolution and at a time when a new landscape for data protection is being redesigned by the draft European Regulation, it is essential for CNIL to conduct a forward-looking strategic activity.

It seemed natural for the smartphone to become the very first topic of the CNIL's strategic planning research, in a world where this device is penetrating ever deeper into everyone's daily life (7 out of ten smartphone users never turn it off!).

The first step of the research involved a status assessment of the practices and perceptions of smartphone users regarding the protection of their personal data. Such was the subject of the survey conducted in November 2011. Its results, analyzed in this Newsletter, have since led to the definition of an action plan. The survey findings indeed revealed a new kind of "privacy paradox": as both a concentrator and a producer of personal data, the smartphone unfortunately remains a 'black box' for its owner, while at the same time a pressing need for data protection is emerging...

Faced with such opacity, our action plan therefore intends among other to analyze in depth and decipher the ecosystem of smartphones, and to anticipate on future usage trends.

Beyond this initial step, CNIL will endeavor to incite the various players in building a framework for more transparent and privacy-friendly products and services.

Isabelle Falque-Pierrotin
CNIL Chairwoman ■

CNIL.

Survey on "Smartphones and Privacy: Uses and Protection Measures"
Smartphones: New Best Friend?

The key findings from the survey[1] (available on CNIL website) reveal that the use of smartphones, while increasingly intensive, is adapting depending on age and socio-economic profiles. While youngsters are obviously attracted by their favorite activities (games, social networking services, instant messaging…), seniors remain attached to the traditional communication functions, although they are already showing an interest for storing their medical data (54% of users age 50 and over). More generally, results show a definite attraction for services relying on a high level of personal data consumption, such as location-based services (55% of respondents).

1. http://www.cnil.fr/la-cnil/actualite/article/article/smartphone-et-vie-privee-un-ami-qui-vous-veut-du-bien/ English version: http://www.cnil.fr/english/news-and-events/news/article/smartphone-and-privacy-best-friends-forever/ Survey conducted in early November 2011 by Médiamétrie Institute on behalf of CNIL, 2315 French smartphone users aged 15 and over.

Geolocation: A new type of sensitive data?

Over 90% of survey respondents wish to choose the times when they are geolocated, to have control over the recipients of their location data, to know how these data will be used and be able to refuse the data transmission. These findings are consistent with the latest survey of CREDOC published in October 2011, focusing on the "Dissemination of ICTs in French Society", and showing that 81% of mobile phone owners wish to have the possibility of prohibiting the transmission of their location data to other companies.

A colossal deposit of personal data…

Three main categories of personal data are "consumed" by smartphones:
- Obviously, contact data and conventional identification data found in any mobile phone, whether "smart" or not. In the case of smartphones, these data are just more numerous and more ubiquitous (e.g. saved in the "cloud"). The user therefore needs to keep control over their access and dissemination.
- Data linked to multimedia contents (photos, videos…) that become omnipresent (86%). A study recently revealed that, in 2011, 27% of all photographs taken in the USA were shot from a smartphone[2]. Yet, such multimedia contents leave traces of behaviors increasingly likely to be compared, enriched, stored, encoded and re-used, in particular via the booming techniques of facial and vocal recognition now publicly accessible.
- Data that are secret by nature (access PINs, bank details, etc.). While their recording into smartphones is less frequent (40% of respondents), they nevertheless raise a real security issue, for instance in case of malware intrusion or illegitimate access to the phone.
It should be noted that, curiously, over 15% of smartphones owners state that they do not store any personal data…

2. NPD study: "Imaging Confluence Study", cited in Wired, December 22, 2011: "How Smartphones Are Changing Photography: The Numbers Are In".

The smartphone, a black box we don't know how to protect

Smartphone owners generally neglect protection measures, due most likely to technical ignorance or to convenience. Thus, over one fourth of survey respondents say they have no locked access code on their phone. And yet – another "privacy paradox" –, 65% of them think that the data stored in their phones are not well protected.
Concurrently, users only have a very vague picture of what business players are doing with their personal data, and a blurred view on their rights: 51% believe that data from a mobile phone cannot be stored or transmitted without their consent, thereby attesting a lack of knowledge on the reality of facts. Numerous studies, including the Wall Street Journal survey on the most popular smartphone apps in the US (*What they know – Mobile*[3]), reveal that large volumes of data are currently transmitted unbeknownst to the users. CNIL intends to develop a number of tools to better comprehend the "concealed economics" of personal data on smartphones, e.g. jointly with INRIA[4] researchers or with the ESPRI project (see Page 4).
Such ignorance is partly due to the fact that the often illegible and incomprehensible terms and conditions of use of services and applications are rarely read by the users (71% never read them). But this lack of knowledge results primarily from the lack of transparency of the market players on the subject. CNIL therefore plans to survey and inventory the "best practices" of market players on issues of information to and control by smartphone users. This issue is of crucial importance for the entire smartphone ecosystem, as shown by the initiatives adopted by GSMA (the global association representing the interests of mobile operators worldwide) on the issue of "Mobile and Privacy[5]" since 2011 (definition of design principles and guidelines). GSMA has already conducted in the UK, Spain and Singapore a poll similar to the CNIL's survey, with similar findings (e.g. showing that 92% of the respondents have concerns about applications collecting personal information without their consent[6]).

3. http://blogs.wsj.com/wtk-mobile
4. INRIA: French Public Research Institute
5. http://www.gsma.com/mobile-and-privacy
6. http://www.gsma.com/articles/gsma-research-shows-mobile-users-rank-privacy-as-important-when-using-applications-and-services/19536

CNIL.

Three questions to... Stefana Broadbent

Stefana Broadbent teaches digital anthropology at University College London. She studies the evolution in uses of new technologies at the workplace and in private life. She recently authored a book on the subject, entitled L'Intimité au travail (2011, FYP éditions, Intimacy at Work).

■ The smartphone is a very intimate, very personal object. For an anthropologist like you, what is special about the prominence that this object has taken in daily life, in the home, in family life?

The smartphone is an intimate object because it provides a continuous and individual link with the people who are emotionally closest to you. This link manifests itself via brief but frequent text or voice exchanges which help maintain a kind of ongoing awareness about the status of your loved ones.

■ Does the smartphone have a specific impact on the split between professional and personal life, on "intimacy at work"?

The major social innovation induced by the mobile phone was to enable permanent contacts with the most intimate social sphere, even from places that used to ban such relationships, like workplaces or schools. When offered the possibility, most individuals will have contacts with their personal social circle from their workplace, whenever they feel the need for it. These new practices have highlighted a paradoxical situation that emerged in the past century: while western societies were developing a culture raising family and intimacy to the rank of a preferred social space – a space providing the comfort, reassurance, subsistence and happiness that the outside world couldn't – people were forced to work in environments that cut them off from such links. Consequently, from an emotional standpoint, individuals were living in a society that overvalued the role of intimate relationships and afforded to the family the ultimate responsibility for taking care of and supporting individuals, even though these same individuals were spending a major portion of their day split off from these relationships. It is therefore not surprising that the mobile phone, as a channel of communication used to reconnect the two spheres, should have been so readily adopted.

■ You often repeat that "80% of our regular exchanges are always done with the same 4 or 5 persons". So, these new technologies do not necessarily broaden our "social network" to the entire world?

Unlike anything that may have been said, individuals have not greatly extended their social networks, and do not spend a lot of time communicating with people far away or encountered in the virtual world. Observations on what users actually do with all the communication channels at their disposal, show intensifying exchanges with a small number of their close relations, which in turn reinforces these relationships.

The four families of French "smartphoners"

An analysis of the survey results has enabled a typology of "smartphoners" to be established, based on their use of mobile Internet and their perception of data protection.

The "carefree" (34%)

The "carefree" have no concerns about the protection of their personal data on their smartphone (they rarely lock it) and feel that their data are protected enough. Their moderate use of the smartphone do not expose them to sensitive or hazardous situations: they store very few secret data, and are less frequently on line than the average smartphone owners. Many "carefree" users do not know that their personal data can be transmitted or recorded without their consent (over half of them think that smartphone manufacturers and operators cannot gain access to their data). This category truly perceives their smartphone as a mere communication tool. They frequently have owned their smartphone for less than two years.

The "casual" (28%)

Just like the carefree, the "casual" are not concerned with the protection of their personal data on their smartphone (95% don't have any access code). However, they are aware that their data are not protected (70%). Compared with average users, fewer of them believe that their personal data cannot be transmitted or recorded without their consent. Overall, this category of smartphone owners seems to find such threats to their data to be harmless and not deserving of any particular efforts to fight them off. This group has a more female and relatively lower socioeconomic status profile.
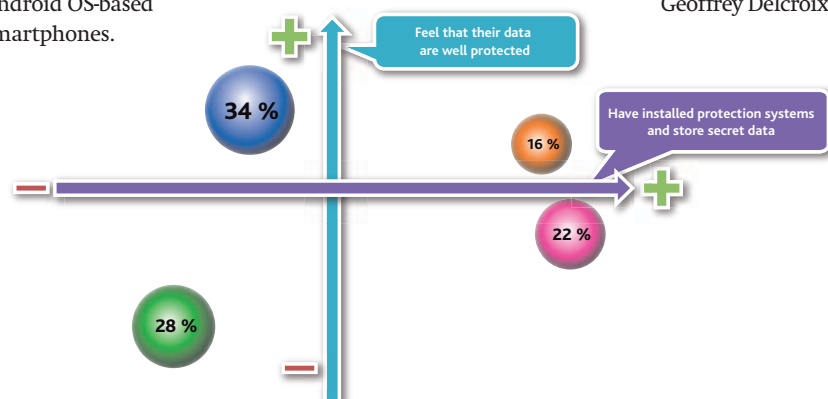
The "paranoid" (22%)

Conversely, the "paranoid" have installed advanced protection systems on their smartphone, but still do not consider that their personal data are properly secured. This feeling of insecurity is encouraged by their storage of high volumes of secret data and by highly advanced uses of their smartphone. The paranoid category includes a majority of men aged 35 to 49, and more frequently than average users, owners of Android OS-based smartphones.

The "confident" (16%)

These individuals show confidence and trust in their smartphones, which they have owned for over two years on average. They store large volumes of secret data, and make extensive use of their phones (virtually all of them download and use applications). They have set up specific locked access systems, and consider their personal data to be well protected. 75% of them believe that their data cannot be transmitted without their consent, and over half think that neither the manufacturers nor the operators can gain access to their stored personal data (versus an average of 42 to 46%). This category includes a majority of male Parisians, with upper socioeconomic status, and one third of them owns an iPhone.

Sophie Vulliet-Tavernier
Geoffrey Delcroix ■

Feel that their data are well protected

Have installed protection systems and store secret data

34 %

16 %

22 %

28 %

CNIL

News in brief...

By 2014, **95%** of the world's population will have one or more mobile phone subscriptions. (Forrester Research, Dec. 2011).

The smartphone application market in the USA is estimated to have generated nearly **20 billion dollars** in 2011. (*How Big is the US App-Economy? Estimates and Forecasts 2011-2015* Appnation and Rubinson Partners, Nov. 2011).

The French "Syndicat National du Jeu Vidéo" (video game trade association) estimates that **12.8 million** users play games on their mobile phones in France (SNJV, *Le jeu vidéo en France en 2011: Éléments clés, Sociologie, pratiques, industrie et tendances*, 2011, www.snjv.org).

Over half of American teenagers on line state that they no longer publish personal information on line due to concerns for their future reputation (*Teens, Kindness and Cruelty on Social Network Sites*. Pew Internet, Nov. 2011).

81% of the French population would like to prohibit the transmission of their location data via mobile phone to commercial companies (*La diffusion des technologies de l'information et de la communication dans la société française*, CREDOC, June 2011).

Only 11% of consumers say that they trust e-merchant sites to keep their personal data secret (KPMG, Dec. 2011).

But **one third** of American teenagers using Internet have already shared their password with a friend or relative... (*Teens, Kindness and Cruelty on Social Network Sites*, Pew Internet, Nov. 2011).

How much are your on-line data worth?

According to a survey published in December 2011 (and cited by L'Atelier among other), conducted with 168 Spanish web users by researchers from the University of Columbia and the Spanish telecom operator Telefonica, web users are relatively well aware of the merchant value of their personal data, but rather opposed to their monetization (source: *Your Browsing Behavior for a Big Mac: Economics of Personal Information Online, 2011*).

This research intended to measure web users' *"attitude and feeling about the collection and monetization of their confidential data when using free online services* (e.g. Google, Facebook...)". The study involved the installation of a plugin in the users' web browser, in order to monitor their browsing behavior, with pop-ups displayed once in a while asking the web user what minimum value they would accept to sell a particular piece of personal information to companies, under a reverse auction system. The major benefit of this research methodology is to demonstrate that an item of personal data has no absolute monetary value in itself, but only a relative value linked to a given usage context.

Researchers found that the most "expensive" data were linked to the user's real identity (age, gender, address, etc.) and those relating to social or financial issues: on average, web users were prepared to sell those data for three times as much as their browsing data. Overall, the replies show that, while web users are aware of the exploitation of their personal data in the context of free online services and find no malicious intent in it, they however feel uncomfortable with the idea that the service providers would take the initiative of monetizing their data.

Geoffrey Delcroix ∎

Exploring issues of privacy via behavior economics

ESPRI (for "Self-exposure, Privacy and Interactive Networks") is a multidisciplinary (economics/sociology/law) project funded by the French Agence Nationale de la Recherche. It is intended to analyze the actual behaviors and practices of service providers and individual users via "field experiments" (quiz on Facebook, fictitious polls, etc.), designed to offset the biases found in declarative surveys. The ESPRI project, coordinated by economist Alain Rallet, involves economists from ADIS[7], jurists from CERDI[8] (two research labs at the University of Paris-Sud) and sociologists from Orange Labs. As an example, one of the ESPRI field trials focuses on the shadow economy of personal data on smartphones. For further information on this project, visit the official ESPRI web site at: **http://www.adis.u-psud.fr/espri**

Geoffrey Delcroix ∎

7. http://www.adis.u-psud.fr/espri
8. http://www.cerdi.u-psud.fr/

Assessment on the web presence of French companies and administrations

Several studies[9] recently provided a highly contrasted view on this subject: low percentage of SMEs present on the Web, gaps in regulations, insufficient professionalism of site design offers, high proportion of sites violating regulations (23% fail to comply with obligations of "legal mentions"), low percentage of web-based transactions using a 3-D Secure payment protocol (11%), large number of "showcase" sites rarely updated (73% of the sites were unchanged for the past year, 91% for three months), inadequate training for public services linked to Internet jobs. Overall in terms of Internet presence, France only ranks in 9th position in Europe and 21st globally. At end 2009, France stood in 11th position in Europe in terms of administrative data available on line, and the satisfaction level for on-line administrative sites remained low (42%). Lastly, telecommuting is three times less developed in France than in the United Kingdom.

Olivier Coutor ∎

9. Eurostat, ICT Usage in Enterprises 2011, March 2011/6th Report of the Cercle d'Outre-Manche, 22 Nov. 2011/E-mail Brokers, consulting firm specialized in e-mail marketing; Baromètre de l'Internet en France, Nov. 2011.