February 2011

CNIL comments on the FTC preliminary staff report « Protecting Consumer Privacy in an Era of Rapid Change »

CNIL, the French Data Protection Authority, welcomes the opportunity to contribute to the preliminary staff report on Protecting Consumer Privacy in an Era of Rapid Change of the Federal Trade Commission (FTC).

CNIL would like to congratulate the FTC for this report that puts privacy at the very heart of companies' business and for its continuous enforcement actions. We welcome its new policy approach and we would welcome a unified privacy framework throughout the United States of America.

When it comes to **new technologies**, we have reached the same conclusions. While recent technological developments (e.g. WiFi, RFID, cloud computing...) are generally good for society, they have also strengthened the risks for individuals' privacy and data protection. To counterbalance these risks, the data protection legal framework needs to be adapted and complemented. Moreover, these technologies have reinforced data transfers by creating a ubiquitous, global and networked world. In this context, **global standards** regarding data protection are becoming indispensable.

While we do not intend to answer exhaustively to the numerous questions raised in this report, we would like to share with you some thoughts and remarks.

I. Privacy framework

1. Scope

We understand that the privacy framework would apply to all commercial entities that collect, maintain, share or use consumer data both offline and online.

While we understand that **government data** and other **specific non-commercial sectors** such as healthcare or human resources are outside your sphere of competence, we regret that a federal privacy framework would not include this type of data – especially in light of the various agreements that are currently being discussed. We believe it is highly important to have a single instrument, as in French law, that would contain general rules applicable to all data – including government data. Of course, specific rules may be established, in particular to limit and adjust certain rights to take into account the specificities of some processing operations, such as for law enforcement purposes. However, we believe such derogations or limitations to the general principles of data protection should be duly justified. As you may know, the European Union seems to be moving towards a similar approach; the European Commission has proposed that the new European privacy legislation encompasses the area of police and judicial cooperation in criminal matters.

We welcome that it should apply to data "*that can be reasonably linked to a specific consumer, computer, or other device*" and not only to **personally identifiable information** (PII). If it were to cover only PII, it would severely restrict the scope of the instrument and

consumers' protection. As you may know, the European data protection legislation[1] has a broad definition of personal data and applies to "*any information relating to an identified or identifiable person*"[2]. Given the perpetual technological developments and the need to adapt to these changes, our national experience teaches us that it is necessary to maintain a broad scope of protection coupled with a technology-neutral and flexible concept of personal data.

Finally, we agree that the four substantive privacy principles you put forward in this report – namely data security, data minimisation, data accuracy and limited retention periods – should be included in business practices. However, other key principles as defined in the OECD Privacy Guidelines and other legal instruments[3] are also relevant (e.g. purpose specification, openness, individual participation (consent, right to access, modify, etc.), accountability...) and should be reflected into the privacy framework and business' practices. In addition, we believe it is equally important to include the protection of international transfer of personal data as a basic element of the privacy framework.

2. Privacy by design and other principles

CNIL has always advocated for the principle of **"privacy by design".** It could be understand as introducing, during the conception of a product, privacy concerns into its functionalities and its process. We believe it should be technologically neutral to remain relevant in a fast changing technological and social environment. It should also be flexible enough to be translated into concrete measures for guaranteeing data protection[4]. This principle should be applicable both to data controllers and to designers and manufacturers of technologies. We therefore very much agree with the FTC approach to "*promote consumer privacy throughout their organisations and at every stage of the development of their products and services*".

Moreover, this development would be in line with the Resolution on "privacy by design" adopted recently by the International Data Protection Commissioners Conference, of which the FTC is a member, and that "*recognizes Privacy by Design as an essential component of fundamental privacy protection*"[5].

Similarly, we fully support **data minimisation** i.e. the requirement to limit data collection to what is strictly necessary. This obligation should also apply to designers and/or manufacturers. Data minimisation would greatly facilitate the implementation of the "privacy-by-design" principle and would make designers and manufacturers aware of their responsibility for the products they circulate on the market. The implementation of the "privacy-by-design" principle should also respect controllability, transparency, user friendly systems, data confidentiality, data quality and use limitation[6].

In addition to promoting Privacy Enhancing Technologies (PETs), we also believe that the protection of privacy could be improved by the setting up of **privacy labels**, developed by

[1] Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[2] See the opinion 4/2007 of the Article 29 Working Party on the notion of personal data - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

[3] E.g. the Convention 108 of the Council of Europe, the Resolution on International Standards of privacy, European directive 95/46/EC

[4] See Article 29 Working Party opinion on the Future of Privacy, December 2009

[5] Resolution on "privacy by design" adopted by the International Data Protection Commissioners Conference in Jerusalem in October 2010

[6] See Article 29 Working Party opinion on the Future of Privacy, December 2009

data protection regulators. For instance, CNIL is currently working on developing benchmarks and precise rules governing the issuance of labels for privacy auditing procedures and trainings. Our first labels should be delivered in 2011.

We also advocate for the **"right to oblivion"** or "right to be forgotten". We believe that it would be unacceptable that information posted on a person remains forever, fixed and intangible, while human nature implies, precisely, that individuals change and are contradictory. This right is critical for the protection of privacy, especially in the online environment, as it would encompass existing principles such the right of deletion, the limitation of the data retention period, etc. It should allow data subjects to withdraw at any time personal data they posted online, hence ensuring that this information would not be detrimental in the future (e.g. right to change one's mind, religion, political opinion, erase youth mistakes...).

In addition to the right to be forgotten, a "**right to data portability"** on the Internet should be introduced. This right to "reversibility" would prevent internet users from being locked in a service; it would thus allow people that do not longer trust a website (e.g. following a change in privacy policy) but that they have used to "archive" their digital heritage, to leave it, and delete all their data, without losing them all as they would get their data back in a standard form.

3. Consumers' choice

We certainly agree that today exercising choice may be very burdensome for consumers. We find your approach to **choice and consent** based on "commonly accepted practices" interesting but we wonder how it may work in practice and whether it might not reduce the level of protection. The paper proposes a two-fold approach: companies should not require consumers' choice "*before collecting and using consumers' data for commonly accepted practices*" and in cases practices require choice, "*companies should offer the choice at the time and in a context in which the consumer is making a decision about his or her data*". It is not clear to us whether the list of "commonly accepted practices" you describe in your paper is exhaustive. In addition, we wonder what happens if a practice falls into a grey area; is the practice interpreted to the benefit of consumers? By whom? For instance, what if a cookie serves various purposes and falls in the two categories of practices? It seems critical and necessary that the lists of commonly and non-commonly accepted practices are elaborated by the FTC, in cooperation with all relevant stakeholders, and bring legal certainty. These lists could be reviewed regularly.

When it comes to **consent**, our experience demonstrates that it is not always an appropriate legitimate ground for data processing. There are many cases in which consent can not be **given freely** - especially when there is a clear unbalance between the data subject and the data controller (for example in the employment context or when personal data must be provided to public authorities) - or **informed**, as the complexity of data collection practices often makes it very difficult for the individual to take knowledgeable decisions[7]. In the field of **behavioural advertising** for instance, current browsers and opt-out mechanisms settings only deliver consent in very limited circumstances as in most cases user's consent is implied if they do not opt-out. Given the nature of these advertising practices, transparency requirements are a key condition for individuals to be able to consent to the collection and processing of their

[7] See Article 29 Working Party opinion on the Future of Privacy, December 2009

personal data and exercise effective choice. The Article 29 Working Party has therefore asked advertising network providers to create prior opt-in mechanisms requiring an affirmative action by the data subjects indicating their willingness to receive cookies or similar devices and the subsequent monitoring of their surfing behaviour for the purposes of serving tailored advertising[8].

As regards your proposal for a **"Do-not-track" list**, we believe a universal mechanism to allow users to manage their preferences concerning the collection of their data for the purpose of behavioral advertising is to be encouraged. However, to be effective this mechanism must be enforceable through precise implementation details, persistent, transparent, and user-friendly.
There are currently several competing proposals to implement such a "Do-not-track" mechanism. For instance, the mechanism proposed by the Mozilla foundation allows the browser to signal to any website (through a HTTP header) that the user does not want to be "tracked"[9]. However, it will only work if it is complied with by websites/advertisers, which could choose to ignore it fully or partially (e.g. still collecting data but not displaying targeted ads). It would thus likely require the FTC to monitor and enforce such a mechanism. Nevertheless, in our opinion, the new routes being explored by the recent "do-not-track" browser-based proposals are more privacy-friendly than the current "opt-out-cookie" mechanism which is largely ineffective.

When it comes to the implementation in practice of a "Do-not-track" mechanism, several questions need to be answered regarding the **choice that is proposed to the user** (is the "do not track" mechanism enabled for all websites, with no exception? is it enabled for all websites, with precise exceptions defined by the user? or is it only enabled for websites chosen by the user?) and **how this mechanism will be enabled by the user** (will the user be asked to enable or disable this mechanism when s/he installs his/her browser? will the "do-not-track" mechanism be enabled by default or will it be disabled by default?)

As regards choice, we believe that the best compromise between privacy and the legitimate interests of websites and advertisers would be a "do-not-track" enabled for all websites, with precise exceptions defined by the user. It would allow the user to receive ads that they consider as relevant from websites/advertisers s/he knows or trusts. In addition, browser privacy settings should offer by default a high level of protection.

As regards **sensitive information and sensitive users**, we believe both should require additional protection. For instance, processing of biometric data in France is subject to prior authorisation by CNIL. In our opinion, sensitive data should also cover categories of data relating to the human body such as genetic data and biometric data but also data relating to certain processing operations of data relating to the localisation of individuals in space (e.g. geographic location).

4. Greater transparency

We agree that practical measures to ensure a greater readability of **privacy notices** and concrete means to enforce consumers' rights are needed. We also believe that "*clearer, shorter, and more standardized*" privacy notices would benefit consumers. Consumers need

[8] See Article 29 Working Party opinion on online behavioural advertising, June 2010
[9] Websites who receive such a signal from a browser are expected to collect no data about the user, and provide not targeted advertising. These websites may however still propose "untargeted" advertising to those users.

to be clearly informed about business' practices, general terms of use and their rights prior or at the latest at the time of collection.

To increase transparency, it is equally important that consumers can **exercise their rights** to access to one's own personal data, but also to object to the collection, to correct, erase or block data, **free of charge**. In the digital age, they should be able to exercise these rights electronically, in particular online, whenever a company runs an e-service. Consumers should retain control over their data.

For instance, the French law provides that an individual is entitled to object, at no cost, to the use of the data relating to him for purposes of commercial canvassing. Data controllers may require payment of a sum of money that may not exceed the cost of a copy of the information, except for requests that are obviously excessive, in particular by their number, or their repetitive and systematic character.
In addition, we believe **maximum time period** should be fixed for the data controller **to answer requests** they receive, according to the complexity of the complaint. In France, the law requires the data controller to answer a complaint within 2 months. If he fails to do so and once the complaint is filed with the CNIL, we usually leave 15 to 30 days, according to the complexity of the complaint, to data controller to answer our requests (complaints in the banking or in the police/justice sectors are generally more complex, thus longer deadlines are granted).

Furthermore, **consumers' education** is also critical. For instance, CNIL just launched an information campaign aimed at young people, school teachers and principals[10]. We also launched on 28 January 2011, the Data Protection and Privacy Day, an iPhone application for young people, downloadable for free, that includes 100 questions on data protection and security on Internet[11].

Finally, we believe that a **national law on security breaches** – both online and offline - would add to transparency and would unquestionably reduce the risks in terms of security.

II. International dimension

Global standards regarding data protection are becoming indispensable. Global standards would facilitate transborder data flows which, due to globalisation, are becoming the rule rather than the exception. As long as global standards do not exist, diversity will remain. Transborder data flows have to be facilitated, while at the same time ensuring a high level of protection of personal data when they are transferred to and processed in third countries. Under EU law, data protection is a fundamental right, protected under Article 8 of the Charter of Fundamental Rights of the European Union. In a globalised world, this means that individuals can claim protection also if their data are processed outside the European Union[12].

The United States of America are a key global player in the field of privacy. We would highly welcome a federal privacy framework that fosters consumers' privacy and that would set high

[10] See our press release (only available in French) : http://www.cnil.fr/la-cnil/actu-cnil/article/article/sensibiliser-les-collegiens-les-enseignants-et-les-chefs-detablissementaux-bonnes-pratiques-su/?tx_ttnews%5BbackPid%5D=2&cHash=f704a7d284
[11] http://www.cnil.fr/english/news-and-events/news/article/with-cnils-app-learn-how-to-surf-the-web-safely/
[12] See Article 29 Working Party opinion on the Future of Privacy, December 2009

standards. We welcome that the FTC became a full member of the International Data Protection Commissioners' Conference and we are confident that the FTC will help in the promotion and adoption of the International Standards on the Protection of Personal Data and Privacy adopted in Madrid in 2009.

We are also looking forward to continuing our **collaboration** with you **on cross-border cases**, in particular with GPEN. We believe it would be a strong message to transatlantic business players if we could develop further coordination actions and carry out joint controls (for instance, on social networks, search engines and behavioural advertising).

In addition, we believe that an international compliance agreement such as the **Safe Harbor Framework** is a valid instrument. We regret however that it is not as efficient as it could be. It should offer redress mechanisms, purpose limitation and companies should actually comply with the level of protection set in the Safe Harbor framework. In addition, we would welcome more transparency regarding the validation mechanisms to obtain certification. We are therefore confident that you will reinforce enforcement actions of the Safe Harbor to enhance the credibility of this key tool for transfers of personal data from the EU to the US.