Privacy: un concetto superato?

Emilie Barrau

Sintesi

Sono in molti a pensare che il concetto di privacy su Internet si possa ritenere ormai superato.

Studi recenti dimostrano che i consumatori europei – inclusi i giovani – prestano molta attenzione alla propria privacy sulla rete (l'82% dei giovani è particolarmente preoccupato del fatto che i propri dati vengano utilizzati senza che ne siano a conoscenza, il 75% che la propria identità sia ricostruita utilizzando dati personali presi da differenti fonti e il 69% che i propri comportamenti siano distorti a causa dei loro dati presenti online).

Tecnologie innovative danno la possibilità agli operatori del settore privato di profilare i consumatori raccogliendo e utilizzando i loro dati personali: ciò porta a un'invasione della loro privacy, spesso senza che questi neppure lo sappiano o abbiano dato la loro approvazione.

Alla Tavola rotonda del 31/03/2009 sull'*Online Data Protection* la Commissaria Kuneva ha dichiarato che i dati personali sono la benzina di Internet e la nuova moneta del mondo digitale.

La Direttiva sui dati personali 45/96/EC costituisce il quadro legale di riferimento per il trattamento dei dati personali nell'Unione europea.

Tuttavia, sia l'entrata in vigore del Trattato di Lisbona sia la Carta europea dei diritti fondamentali sia la Convenzione europea dei diritti umani riconoscono la tutela dei dati personali e il diritto alla privacy quale diritto fondamentale, quindi rafforzano la tutela.

Inoltre non è da sottovalutare il ruolo che la legislazione "tradizionale" (la Direttiva sulle pratiche commerciali scorrette e quella sulle clausole abusive) può ricoprire per la tutela della privacy dei consumatori.

È risaputo, per esempio, che molti *privacy policy* non rispettano i requisiti-base sulla trasparenza: la maggior parte dei consumatori non legge abitualmente le condizioni sulla privacy riportate nei contratti a causa della loro lunghezza, complessità di scrittura e conseguente difficoltà di lettura. Questo comporta il fatto di non conoscere i propri diritti da parte dei consumatori all'atto di sottoscrizione dei contratti.

Il fatto che i consumatori non esercitino i propri diritti non significa che non abbiano a cuore la propria privacy. Dimostra piuttosto la necessità di modificare i contratti che gli utenti devono sottoscrivere: migliorare le condizioni generali e semplificarne l'accessibilità utilizzando un linguaggio semplice

Emilie Barrau
Beuc, Bureau Européen des Unions de Consommateurs
Sintesi a cura di ***Luisa Crisigiovanni***
Altroconsumo
Associazione Indipendente di Consumatori

e appropriato, che consenta loro di autorizzare con consapevolezza il trattamento dei propri dati.

Se da una parte è importante considerare il fatto che esistono numerosi strumenti di controllo del processo di raccolta dei dati personali, dall'altra sono molti i casi di infrazioni in tale ambito che restano non sanzionati.

Il modo migliore per aumentare la tutela dei consumatori è assicurare che possano esercitare i loro diritti con semplicità e a tutti i livelli.

Campagne di informazione relative alla tutela dei propri dati personali dovrebbero essere organizzate dalle associazioni di consumatori e dalle autorità nazionali.

Tuttavia se è vero che informazione ed educazione aumentano la gestione consapevole della propria privacy, è anche vero che non si deve scaricare tutta la responsabilità sulle spalle del consumatore:

- si deve migliorare la modalità di comunicazione sulla privacy online da parte delle imprese;
- si dovrebbe introdurre il rispetto della privacy in modo standard nel design stesso dei programmi informatici, così da facilitare le procedure di verifica e di notifica da parte delle autorità di controllo;
- tutti gli attori coinvolti dovrebbero condividere la responsabilità nell'assicurare che i dati in circolazione siano stati raccolti e utilizzati in sicurezza e avere regole trasversali per la loro gestione, non solo nel settore della comunicazione elettronica;
- i consumatori dovrebbero essere risarciti per qualsiasi danno dovessero aver subìto a causa di inadempienze relative all'utilizzo dei dati personali o all'utilizzo non autorizzato. A tale proposito si auspica l'introduzione di uno strumento di azione collettiva (*group action*) in Europa;
- infine sarebbe opportuno introdurre nuovi diritti specifici relativi al mondo digitale per garantire una maggiore tutela dei consumatori: il diritto all'oblio e quello alla portabilità dei dati.

Chi pensa, dunque, che l'epoca della privacy sia ormai superata è probabile che senta parlare di privacy online ancora per molto, molto tempo.

Introduction

Facebook founder and Ceo Mark Zuckerberg recently stated that the age of privacy on the Internet is over and that users should get over it... but should they?

Recent studies show that European consumers - including young people - do care about their privacy online.[1] *Moreover, as a recent announcement on data retention from a major online player demonstrates, privacy is also seen as a competitive advantage and - let's be honest - a proof of good will when it comes to regulators' scrutiny.*

*I am convinced that online privacy is not going to fade away especially as «*personal data is the new oil of the Internet and the new currency of the digital world*»*[2]*. Technological evolutions, new business opportunities as well as new consumers' online behaviours, create challenges that will have to be addressed be it at national, European and/or international levels.*

Far reaching changes have occurred in the way consumers' data is accessed, processed and used online; every single activity online leaves a digital footprint. The online environment results in new and unprecedented risks to privacy which cannot be compared to those occurring offline.

New technologies (including behavioural advertising, email-scanning and deep packet inspection techniques) and new digital content platforms (for example social networking sites or micro-blogging sites) in particular allow players from the private sector to profile consumers by collecting and using their personal details and invading their privacy without their knowledge or approval. The same data is also exposed to online crime, such as ID theft and/or the diversion of sensitive information.

The current developments are likely to be decisive in the development of the Internet of the Future also referred to as "the Internet of Things" i.e. the integration of information and communications technology (Ict) into the environment and everyday objects. Due to mass storage technologies and the increasing connectivity of databases, the Internet of Things will exponentially increase the possibilities of tracing and tracking consumers. The multiplication of information collection from objects, readers, tags, sensors... everywhere - from the workplace, through public transport, and within individuals' homes - will facilitate this operation.

It is therefore important to set up the right framework and address the relevant challenges today to shift control back into consumers' hands. Loss of privacy should not be considered as a collateral effect for using the Internet.

[1] A recent scientific report demonstrates that 82% of young people are very concerned that personal information is used without their knowledge, 75% that their identity is reconstructed using personal data from various sources and 69% that their views and behaviours may be misrepresented based on their online personal information. see Scientific report "Young People and Emerging Digital Services", 2009: http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=2119.

[2] Commissioner Kuneva, Roundtable on Online Data Collection, Targeting and Profiling, 31 March 2009.

The European legislative landscape

First of all, it is important to acknowledge the changes that will be brought by the Lisbon Treaty. In fact, both the European Charter of Fundamental Rights and the European Convention on Human Rights recognise the protection of personal data and the right to privacy as fundamental rights. Therefore, those rights will need to be fully complied by both the European institutions and Member States, acting within the scope of Eu law.[3] *In addition, Commissioner Designate for Justice, Fundamental Rights and Citizenship, Viviane Reding, has proposed to analyse, with a specific impact assessment on fundamental rights, whether all European Commission proposals are in line with the European Charter.*

The Data Protection Directive 45/96/EC, a technology-neutral instrument, constitutes the fundamental legal framework governing the processing of personal data in the Eu. This piece of legislation consecrates, amongst others, the principles of transparency of data collection, fair and lawful processing, purpose limitation and specification, data minimisation, consent, and the right to access, object, correct and withdraw one's data. In addition, the Directive 2002/58/EC on privacy and electronic communications, the so-called ePrivacy Directive, which was recently revised,[4] *completes the legal regime with respect to the processing of personal data in the electronic communication sector.*

*It is also worth noting that lately several technologies/sectors have captured the European Union's attention. For instance, the European Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (Rfid) was developed to help Member States to implement Rfid applications in a «*lawful, ethical and socially and politically acceptable way, respecting the right to privacy and ensuring protection of personal data*». Similarly, the issue of online data collection - and in particular targeting and profiling of consumers - has risen on the political agenda of the European Commission. It is likely that the new Commission will come forward with initiatives in this field.*

Finally, one should not forget that poor data protection or privacy practices often come in the shape of unfair contractual terms or unfair commercial practices. The role of "traditional" consumer protection law as a means to protect consumers' data protection and privacy should not be underestimated. For instance, the Unfair Commercial Practices Directive and the Directive on Unfair Contractual Terms could play a role in ensuring that online profiling and targeting marketing techniques are fair to consumers.

[3] The Uk and Poland opted out of the European Charter.

[4] ePrivacy Directive was part of the so-called "Telecom Package" that was adopted in November 2009. The new rules have to be transposed into national laws of the 27 Member States by June 2011.

Identifying the pitfalls

The European Commission recently launched a consultation on the review of the general data protection framework to see whether the current legal framework meets the new challenges for personal data protection in the light of new technologies and globalisation.

Since the adoption of the Data Protection Directive, the rapid development of the information and communications technology together with the development of new services, raise a number of challenges as to the practical application of the principles of the Directive to the online environment.

For instance, many privacy policies of online service providers do not abide by the compulsory transparency requirements.[5]

Did you know that the average reading rate is between 200-250 words per minute? If you take Bing MSN terms and conditions (14.223 words) for instance, it would take an average reader more than one hour to read them. Similarly, it would take an average reader almost 25 minutes to read Twitter terms and conditions (5.563 words).[6] *And this is just the time it would take to read the terms and conditions - not even to try to understand what they mean.*

Today, the vast majority of consumers do not currently read privacy notices due to their length, complexity and complicated wording. The notices fulfill legal business obligations rather than informing consumers. They are not always easy to spot on a website nor in a language the consumer can understand. Consequently, consumers just give up and do not know what they are agreeing to.

Similarly, while it is important to note that there are several ways to validate the processing of personal data, the requirement to obtain users' "free, informed and specific" consent, wherever relevant, is frequently infringed in the online environment.

Also, many Internet companies do not always comply with the principles of purpose limitation and the specification of use of personal data or acknowledge the rights of data subjects to access, object to or erase their personal data.[7] *Some companies even claim that they own or have a perpetual licence to use the content uploaded by the consumer to their website.*

The current practices lead to an erosion of consumers' rights online and an increasing trend towards asymmetry of information and data centralisation, resulting in the shift of control away from consumers.

Addressing the challenges to achieve consumers' empowerment

It cannot be inferred that consumers do not care about their privacy simply because they do not exercise their rights. In fact, how do you want consumers to

[5] Articles 10 and 11 of the Data Protection Directive 45/96/EC.

[6] Consumer Council of Norway study on social networking sites terms and conditions.. http://forbrukerportalen.no/filearchive/matrix_terms.jpg.

[7] Articles 6 and 12 of the Data Protection Dir. 45/96/EC.

evoke their rights when they do not know in the first place that their data are being collected and processed?

First of all, fairness of terms needs to be improved and policy notices must be easily accessible and clearly displayed in plain and intelligible language. Notice must be provided at the point of collection. Several options could be explored to improve transparency such as the use of layered privacy notices i.e. first providing the user with a summary of key privacy points, and then providing access to the full privacy policy for those who wish to access more detailed information, or the development of notification standards by data protection authorities.

Therefore, the best way to achieve consumers' control is to ensure that consumers can exercise their rights easily and at various levels. In the online world, consumers should have the possibility to exercise their rights freely and by email/ via electronic means - and not by snail mail as it is most often the case today, which creates an asymmetry of rights/duties and an extra burden on the data subject. In addition, privacy campaigns should also be run by consumer organisations and data protection authorities to raise awareness amongst consumers about their rights and obligations. However, it is important to note that while there is a role for better information and education of consumers, one should be careful not to put the full responsibility on consumers' shoulders. All stakeholders, and in particular businesses and enforcement authorities, have to do their share of the work to achieve a balanced online environment.

Next, we firmly believe that privacy and security by design - i.e. building security and privacy from the very beginning in the design specifications of systems and technologies and from end to end - is a necessary additional tool to foster trust, to empower users and to ensure accountability. "Appropriate technical and organisational measures" are already required in the Data Protection Directive.[8] Such technical solutions could foster consumer control and facilitate consumer choice. Privacy by default would also help comply with the principle of data minimisation, data security and would facilitate the notification and verification procedures by the Data Protection Authorities (DPAs). In addition to the use of technical solutions, we believe that Privacy Impact Assessments (PIAs) and audits/controls should be made compulsory for both data controllers and data processors.

Despite the obligation on the data controller to take appropriate security measures to protect the data they store, more and more data breaches make it to the front pages of newspapers. We are convinced that more accountability of the various online players will work towards better and fairer practices. This is why we believe that all actors should have a share of responsibility in ensuring that the data which circulates is being collected and processed, is secured and that horizontal rules concerning the prevention, management and reporting of data breaches - not just in the electronic communications sector - are needed.

Moreover, business should also compensate consumers for any detriment they may suffer as a result of data breaches or unauthorised use of data. Given the

[8] Article 17 and Recital 46 of the Data Protection Directive 45/96/EC.

relatively low amount of money involved in such cases and the fact that moral damages are difficult to quantify, consumers will not go individually to court. A collective judicial redress instrument ("group action") in Europe will ensure that consumers can exercise their right to be compensated for the damage they have suffered. If such a measure existed, it would also provide an incentive for companies to abide by the law.

Finally, we also consider that Data Protection Authorities (DPAs) must be given the means and the tools to fulfill their mission. They should be independent, have the technical competence, sufficient powers and adequate resources to control and sanction. In addition, one should reflect on the role consumer protection authorities could play as additional enforcers.

Introducing new consumers' digital rights

New rights specific to the Digital Age should be introduced to better protect consumers' privacy online: the right to be "forgotten" and the right to data portability.

Everything posted online may stay there for perpetuity, in some form or another - through Internet archives websites or search engines caches[9] - even posts or pictures one thought no longer existed. This is even more relevant for young people; would they want appalling photos taken at parties[10] years earlier popping up on the Web to be seen by their future employer?

We believe that a general right to "be forgotten" i.e. a right to have one's data deleted for good on the Internet should be introduced. A draft law[10] currently being discussed in France is looking into making such a right - "droit à l'oubli" - *effective in practice.*

Second, consumers are increasingly "locked-in" to certain online sites and social network sites and it is not easy - if not impossible - to change from one service provider to another, due to all the messages/pictures/e-mails/videos one has stored. Right to data portability should be understood as the right to recover and/or to shift from one platform/cloud to another data posted (e.g. photos). In our opinion, it is clear that consumers should retain the ownership of data posted online. Existing terms and services appear mostly to be unfair and should be changed accordingly. In addition, for this right to be effective, interoperability between services is required.

To sum up, a consumer's right to privacy should not be undermined or mitigated merely because it has become easier and more profitable to break it in the virtual world. Whether you believe that the "social norm" has changed and that the age of privacy is over, or on the contrary, that it is high time to reestablish barriers as you are able to do in the physical world, you may still hear about online privacy for a little while.

9 "*Privacy by design... take the challenge*", by Ann Cavoukian, Ontario Information and Privacy Commissioner, 2009.

10 Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure numérique, November 2009.