Big brother is -still- watching you

Marina Rigou, Panteio University

The Internet, based on the convergence of computers and telecommunications, has become the core of today's digitized and globalized world. About 2.3 billion people around the world are Internet users or in other words one third of the world's population is using the Internet[1]. In the European Union[2] internet penetration has reached the 71.5%[3] of the population and in the USA the 78.3%[4]. It's obvious that not all are members of the information society. The gap between "inforich" and "infopoor" countries and people still exists, but I would like to mention that in 2001 internet users per 100 inhabitants in the developed world were 29.4 while the same statistic value in the developing world was 2.8. Ten years later the developed world increased by 2.5 times the number of internet users while developing countries increased 9.4 times the same number. But internet users in developing countries were still just 26.3 per 100 inhabitants.

Nevertheless the Internet is still growing at a good rate, contributing to a communication revolution. Time and space has been demolished in the cyberspace and gradually the Internet became an instrument which changed the everyday life and affected the social, political and economic fields. Individuals use the medium of the media -as Internet could be consider- not only for communication and entertainment but for social, economic, political, commercial, business and search activities. Additionally the Internet is used to accomplish transactions between citizens and the state or other services leading in this way to compulsory internet use[5]. The adoption of the Internet by governments, politics and public services as a means to bring forth their activities and communicate with people induces a sense of visibility, but as Foucault has mentioned is a trap[6]: Not only because -as the French philosopher has said- it is through this visibility that modern society exercises its controlling systems of power and knowledge, but it is that this visibility is bilateral and in fact, is a semi-visibility. Bilateral because as exercise of political power is subjected to a kind of

[1] http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf
[2] In Europe, internet penetration is 61.3% (http://www.internetworldstats.com/stats4.htm) and in China 38.4% (513 million people, 50.5% of Asian users) (http://www.internetworldstats.com/stats3.htm). In Greece 46.9% (http://www.internetworldstats.com/stats4.htm)
[3] http://www.internetworldstats.com/stats9.htm
[4] http://www.internetworldstats.com/stats14.htm
[5] For example to submit tax declaration or to use other online government services.
[6] M. Foucault, *Discipline and Punish: The Birth of the Prison*, Vintage Books, New York 1979 p. 200

scrutiny which simply did not exist before, in the same way citizens are exposed to visibility leaving a very large public footprint which constructs a far more detailed portrait of the individual than those recorded at any time in the past. Furthermore, information about individuals is no longer under the control of the person to whom the information pertains and such loss of control is loss of privacy. On the other hand ambiguous politics would never been made deliberately public. It's only after journalistic or other investigation that risky or unlawful decisions and acts become known. But even so, by the pressure of publicity, citizens exercise a kind of power.

The Internet expansion was supported by the broadband connections which as a result had the evolution of Web 2.0, an environment in which uploading content became easy and fast. Social networking websites attracted millions and eventually the notion of privacy has changed. "Privacy is the right to autonomy, and it includes the right to be let alone. Privacy encompasses the right to control information about ourselves, including the right to limit access to that information. The right to privacy embraces the right to keep confidences confidential and to share them in private conversation. Most important, the right to privacy means the right to enjoy solitude, intimacy, and anonymity (Flaherty 1989, p.8)" [7]. However users tend to upload everything about their lives without considering the consequences of such an act. Even the most intimate thoughts could be seen blogged transforming cyberspace into a psychoanalytic couch. Of course this is not the rule. In Europe[8] 74% of the users see disclosing personal information as an increasing part of modern life. But simultaneously 70% of Europeans are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected and they think that they have only partial, if any, control of their own data. It is interesting that personal information is considered, above all, financial information (75%), medical information (74%) and national identity numbers or cards and passports (73%) with a percentage around 74%. Sixty per cent of users purchase goods or services online and 52% use a social networking site. The use of search engines is a dominant activity which exceeds 80%. In the US two in three online adults (63%) say

[7] Whitfield Diffie and Susan Landau, *Privacy on the line*, The MIT Press, Cambridge, Massachusetts 2007, p. 142

[8] Special Eurobarometer 359. *Attitudes on Data Protection and Electronic Identity in the European Union*. Fieldwork November-December 2010. Publication June 2011. For the Greek case Lilian Mitrou, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments-Greece*, May 2010.

they currently maintain a profile on a social networking site[9], 91% use a search engine to find information and about 70% purchase goods or services online[10]. But every click users make for these and others internet activities, leaves footprints.

In this context, full of value information and easy to be accessed in the digital era transformed cyberspace to a new gold mine and digital digging for information became business. Sites feed personal details to a new tracking industry. Information about online browsing habits, purchasing behavior, and other online activity is collected, analyzed, combined with other online or offline information, used and shared, often instantaneously and invisibly. Tracking technology is getting smarter and more intrusive. Cookies, flash cookies and beacons are the digging tools.

Cookies are small text files, installed on a user's computer by a website, that assign the user's computer a unique identity and can track the user's movements on a site. Beacons are bits of software code on a site that can transmit data about a user's browsing behavior, they are more powerful than cookies and can record a person's keystrokes online. Flash cookies are used in conjunction with Adobe Systems' Flash software, which is widely used to display graphics and video on websites. They are useful because they can "remember" the settings used by the user last time but they can also re-spawn trackers that a person may have deleted. These "tracking files represent the leading edge of a lightly regulated, emerging industry of data-gatherers who are in effect establishing a new business model for the Internet: one based on intensive surveillance of people to sell data about, and predictions of, their interests and activities, in real time"[11].

So new "tools" scan in real time what people are doing on a Web page, then instantly assess location, income, shopping interests. Coming to medical conditions or even more to politics this procedure is really dangerous. For example in Iran since President Mahmoud Ahmadinejad's disputed re-election on June 2009 the power of social media has been of enormous help in organizing demonstrations in favor of Mir Hosein Mousavi. But this was the one side of the coin. The other side lies in the Iranian prisons. Digital footprints were followed by the regime's security forces. And

[9] *Privacy management on social media sites*, Pew Internet, February 24, 2012, http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx

[10] *What Internet Users Do Online*, Trend Data (Adults), Pew Internet, March 2000-February 2012, http://www.pewinternet.org/Trend-Data-(Adults)/Online-Activites-Total.aspx

[11] http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html#project%3DCOOKIESLIDE1007%26articleTabs%3Darticle

as in Iran, in China and in other authoritarian countries cyber-dissidents face the peril and the reality of jail. The world's largest netizen prison is in China. The emerging general trend is that a growing number of countries are attempting to tighten their control of the Net, but at the same time, increasingly inventive netizens demonstrate mutual solidarity by mobilizing when and where necessary. The outcome of the cyber-war between netizens and repressive authorities depends upon the effectiveness of the weapons each camp has available: powerful filtering and surveillance systems for decrypting e-mails, and ever more sophisticated proxies and censorship circumvention tools such as Tor[12], VPNs[13], Psiphon[14], and Ultra Surf[15]. The latter are developed mainly thanks to the solidarity of netizens around the globe. For example, thousands of Iranians use proxies originally intended for Chinese surfers.

On the other hand, search engines that offer e-mail services -such as Yahoo or Gmail- retain the personal information users are required to enter when opening an e-mail account. Social networking websites allow advertisers too much access to their users' behavior and data. And users have no control over all their personal data and the right to be forgotten is really forgotten. Surveillance empowered by technology violates privacy and in some cases the cost is larger than the violation of a fundamental right.

---

[12] Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis. https://www.torproject.org/

[13] A virtual private network (VPN) is a private network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet. VPNs provide security through tunneling protocols and security procedures such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a head office network through the public Internet. http://en.wikipedia.org/wiki/Virtual_private_network.
See also http://www.vpnc.org/vpn-technologies.html

[14] Psiphon is a set of technologies that use a combination of secure communication and obfuscation to defeat network censorship systems. All Psiphon software is open source and designed to circumvent politically-motivated Internet censorship in countries where such censorship is extra-legally enforced.
Psiphon is not designed for strong anonymity, avoidance of copyright, or to allow users to share pirated software, unlicensed audiovisual material, or to access illegal content such as child pornography. We are governed by the laws of Canada, and abide by best practices in ensuring user safety and privacy. http://psiphon.ca/

[15] Ultrasurf is a product of Ultrareach Internet Corporation. Originally created to help internet users in China find security and freedom online, Ultrasurf has now become one of the world's most popular anti-censorship, pro-privacy software, with millions of people using it to bypass internet censorship and protect their online privacy. PRIVACY: Protect your privacy online with anonymous surfing and browsing. Ultrasurf hides your IP address, clears browsing history, cookies, and more. SECURITY: Using industry standard, strong end-to-end encryption to protect your data transfer from being seen by third parties. FREEDOM: Bypass internet censorship tobrowse the internet freely. http://ultrasurf.us/

A Wall Street Journal investigation[16] has found that the largest U.S. websites are installing intrusive consumer-tracking technologies on the computers of people visiting their site, in some cases, more than 100 tracking tools at a time. Some two-thirds of the tracking tools installed (2,224) came from 131 companies that, for the most part, are in the business of following Internet users to create rich databases of consumer profiles that can be sold. The companies that placed the most such tools were Google Inc., Microsoft and Quantcast Corp., all of which are in the business of targeting ads at people online.

To measure the sensitivity of the data gathered by tracking companies, the Journal created an "exposure index" for the top 50 sites. Dictionary.com ranked highest in exposing users to potentially aggressive surveillance: It installed 168 tracking tools that didn't let users decline to be tracked and 121 tools that, according to their privacy statements, don't rule out collecting financial or health data. Dictionary.com attributed the number of tools to its use of many different ad networks, each of which puts tools on its site.

Some of the tracking files identified by the Journal were so detailed that they verged on being anonymous in name only. They enabled data-gathering companies to build personal profiles that could include age, gender, race, zip code, income, marital status and health concerns, along with recent purchases and favorite TV shows and movies. The ad industry says tracking doesn't violate anyone's privacy because the data sold doesn't identify people by name, and the tracking activity is disclosed in privacy policies. But it is clear that there is a systematic effort by companies to gather data with which it could be possible to identify the digital with the real identity by data matching. Where traditional businesses generally collect information about customers from their purchases or from surveys, internet companies have the luxury of being able to gather data from everything that happens on cyber sites. As David Lyon says "Orwell's dystopic vision was dominated by the central state. He never guessed just how significant a decentralized consumerism might become for social control"[17]. Big Brother is still watching us and the legal framework is facing real challenges as it tries to follow the rapidly changing technology and the differences across borders.

[16] http://online.wsj.com/article/SB10001424052748703977004575393121635952084.html
[17] David Lyon, *The Electronic Eye: The Rise of Surveillance Society*, University of Minnesota Press, Minneapolis 1994

“Cloud computing” could also pose challenges to data protection, as it may involve the loss of individuals’ control over their potentially sensitive information when they store their data with programs hosted on someone else’s hardware. Geolocation, the WiFi data processing and the Google Earth enhanced with ‘live’ steaming view are some more cases of personal data collection. So the European Union and the United States face similar challenges regarding privacy. The common place is the perception of the cyberspace as a digital single market. To flourish digital economy needs trust and trust is all about the confidence citizens have when giving personal information online. On both sides of the Atlantic are currently working on new laws in the field of data protection. The Safe Harbor agreement for commercial activities, where personal data transferred from Europe benefits from privacy protection across the Atlantic, is the first step for European and US co-operation on the protection of personal data. The US is assessing its approach to privacy which in general is more in favor of industry self-regulation structure based on five core principles: 1. Notice/Awareness; 2. Choice/Consent; 3.Access/Participation; 4. Integrity/Security; and 5. Enforcement/Redress. The EU also has decided to clarify and modernize its data protection legislation. The Commission will propose one, single, technologically neutral and future-proof set of rules across the EU. This means that regardless of how technology and the digital environment develop in the future, the personal information of individuals in the EU will be secure, and their fundamental right to data protection respected. Whenever consent is required for data processing, it will have to be given explicitly, rather than be assumed. The Commission will also reinforce the ‘right to be forgotten’, so that if an individual no longer wants their personal data to be processed, and there is no legitimate reason for an organization to keep it, it must be removed from their system. Citizens will also have a right to data portability, i.e. the right to obtain a copy of their data from one Internet company and to transmit it to another one without hindrance from the first company. ‘Privacy by design’ and ‘privacy by default’ will also become essential principles in EU data protection rules. This means that data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm –for example on social networks. National data protection authorities will be strengthened so they can better enforce the EU rules at home. These are some of the changes that the new legal framework will include. Although it is said to be a future-proof set of rules which will take into account the most recent technological

developments, it is difficult to say how full proof it will be and for how long, as technology is unpredictable and always a step ahead of the law. And we must be aware of the peril that an absolute market and digital economy orientation could lead to the slackening of the legal framework of the privacy rights protection.