FAIFE SPOTLIGHT

Sleepwalking toward a control society? Ten Must-Know Trends

Kai Ekholm & Päivikki Karhula

Contents

1. “Free internet is dead" - global conditions of control has been established

Boundaries of surveillance and censorship have changed during the history of Internet. The idealism of Internet as a separate open and free space labeled the beginning of the Internet era in mid 1990s. Up until the end of the decade most states either ignored online activities or regulated them very lightly. Since the beginning of 2000s development turned towards continuous increase in forms of control which also became more subtle and nuanced. (Deibert et al. 2011).

Censorship and data surveillance have become a globally accepted condition. In 2010, more than 60 countries censored the Internet, and many countries have passed a law that sets restrictions on citizens and media's freedom of expression (Reporters Without Borders 2011). Targeting of control to individuals has also improved, since several states require identification, licensing or registration from the users on the Internet (Palfrey 2010). In many countries even the protection mechanisms of users, like encryption, are reduced to prevent users protect their communications (La Rue 2011).

Different forms of control are increasing in scale, scope and sophistication around the world, and both in democratic countries and authoritarian states (Bitso & Fourie & Bothma 2012). Although Arab Spring indicated that Internet and social networks can be efficiently used also as vehicles for freedom, repressive regimes soon responded with tougher measures of control. Internet content filtering is still growing, but Internet surveillance is growing even more and getting more intrusive. (Reporters Without Borders 2012)

Internet control has taken various forms and measures in different countries. Reasons for censorship, methods of control, censoring parties and sanctions about the exceeded limits differ largely. Severity of the conditions the control mechanisms develop varies from pervasive forms control and heavy sanctioning of violations in totalitarian countries to milder forms of censorship and permissiveness of the critics of controls, which often takes place in western democracies. Legal framework, state of Internet infrastructure, level of economic development and the quality of governance seem as key factors in determining how models of internet control are implemented. (Bitso & Fourie & Bothma 2012)

The presently strictest and large-scale structures of control are in China. Using China as an extreme example, Jevgeni Morozov, in his important book The Net Illusion, shows how dictatorships effectively use the net against their citizens. China has hired 20.000 cyber police officers to observe the citizens' use of the net. "Human search engines" literally go and get the opponents of the regime from their homes to be held liable for their words. An elderly villager once criticized the government on the net for polluting a river, and he was fetched from his home and forced to take responsibility for his words. (Morozov 2011)

In Europe, the most recent countries that have fallen back on censorship are Hungary and Turkey. In Turkey, all Internet users were obliged to use a mandatory net filter. Only 22.000 of the total 11.5 million net users have adopted it. (Reporters Without Borders 2012)

Governments are the most important enforcer of internet censorship (Bitso & Fourie & Bothma 2012). However, vast part of the cyberspace is owned and operated by private sector; when governments want to extend their control over the Internet, they have placed greater demands on private sector actors to police and secure communications (Deibert, 2012). Accordingly, many of the censoring and surveillance efforts are based on public-private partnerships. Also, private companies have significant power on the Internet due to their size: Google, Facebook, eBay, Amazon are among the private multinational corporations which are major players on the Internet (Hamilton & Moon 2012).

There is no clear division between totalitarian and democratic countries, or between intentions of public and private sector actors in relation to the outcomes of their censoring efforts. The public-private censorship partnerships have produced large-scale structures of control, but also companies from democratic countries have worked for the totalitarian governments. The Great Firewall in China has been built up by the support of major western ICT-companies, including Cisco, Microsoft, Yahoo and Google (BBC News 2010). In Europe, it has appeared that ICT-companies have sold surveillance technology to human rights-violating governments in countries like Egypt, Libya, Syria and Iran. These technologies have been used to track the activities of dissidents, human rights activists, journalists, student leaders, minorities, trade union leaders, and political opponents, but they may have been employed to monitor entire populations. (Privacy International 2011a)

Overall, the major players of Internet whether they are government bodies or private parties, have proofed that they have power to close or open the doors into the networked environment and its' services, if they wish so (Hamilton & Moon 2012). Whether this is done in a long run to the benefit of the civil society and to support freedom of information or against it, still remains as an open question – so far the political will has changed in different cases.

2. Western countries have resorted to excess of justifiable defense

Western democracies certainly do not have same political or religious grounds behind the increased use of control mechanism than totalitarian countries. Democracies have extended their surveillance and censorship practices by grounds like national security, threat of terrorism, crime detection and border and immigration control (Gschrey, 2011, O'Brien 2010). In the aftermath of 9/11, many states have established large-scale control mechanisms and enacted the most stringent and the most restrictive privacy threatening laws in the post-war period (E.g. Bloss 2007, EDRI 2011, EDRI 2012). According to

Freedom of Expression organizations, such as the Privacy International and Electronic Privacy Information Center, the UK and the USA have become societies of strong social control (Anderson 2007).

Tools of control are built increasingly on the level of infrastructures of the Internet (Deibert et al. 2011). Since 2001, the world has seen a massive build up of preventive data control systems on a global level, and international data transfer protocols; the PNR transfer in the USA and in the EU, for example (Cohen 2012, Privacy International 2004). Presently, backdoors for exceptional uses of governments are built in the information architecture of networks; and these requirements may be based on laws and international standards (e.g. ETSI) (Baloo 2004, Cross 2010).

Infrastructural control is very non-transparent, but it may have global impacts. Surveillance which is built in to the information architecture paves the way for any powerful party to gain a global access on data flows. While Internet's architecture supports mechanisms of control, they can be exploited in the policies of governments and businesses (Hamilton & Moon 2012).

Justifications to extended control mechanisms have also become supported by legislation. Many exceptional procedures and emergency legislations have changed as a permanent practice; Patriot Act is in USA is a good example of the laws, which was compiled as an emergency legislation, but it has been now in force over 10 years (Goldberg, 2012). Since countries are influenced by each others' policies and situations, legislative models may have a wider influence (Bitso & Fourier & Bothma 2012). Especially, U.S. models and justifications for control require attention, since their impact may spread largely through the practices of multinational companies and international agreements. U.S. based multinational corporations are among the major players on the Internet. Also, USA has gained a leading role in globalized approach to surveillance (Mueller 2010).

Extended monitoring of citizens, which has been based on different grounds (e.g. national security, copyright violations) and legislative changes has exceeded civil rights, set forth restrictions to free flow of information and neglected the social impacts of control mechanisms (Carey-Smith & May 2006, EDRI 2011). In USA, especially developments past 9/11 have accelerated unprecedented surveillance, search and seizure authority (Bloss, 2007).

Moreover, technologies alone may override civil rights, since they can establish large-scale mechanisms of control without political debate or consent of users. Standard based mechanisms bind developers of technologies commonly implement the tools of control into the basic structures of the Internet. However, it is difficult to point out any one Big Brother who would have intentions to use these mechanisms. Consequently, these kinds of forms of control stay hidden from public and political discussion and become neutralized in relation to the purpose of their use. Practices like use of backdoors, forced identification, data collection and locating and monitoring users and their communications have already largely been applied without public discussion or users' consent.

3. Complexity of Internet censorship and data surveillance

During the classical period of censorship, the control focused on publications or writers. On Internet methods of control do not only involve in contents, but they may involve in users communications within the infrastructure of Internet (La Rue 2011). Censorship often goes hand in hand data surveillance. There are also social and economic measures of control, which have censoring effects, like pricing, forced identification or registration, unavailability of internet connections and pressure for self-censorship (Bitso & Fourie & Bothma 2012).

Filtering is a most common form of internet censorship. From a point of view of access users may be restricted by regulating 1) the user's access to the network; 2) the user's access to a particular service (DNS-filtering); 3) the user's access to a specific site (IP-filtering); 4) the user's opportunity to see certain web-pages (URL-filtering) or 5) filtering based on keywords of content (keyword filtering) (Bitso & Fourie & Bothma 2012). Also censorship and data surveillance may be combined; monitoring of data recognizes the given problematic contents - and operations and methods of censorship can be targeted for these findings (Dutton et al. 2010).

Intermediaries, like ISPs (Internet Service Provicers), generally describe actors who provide connections or services on Internet (EDRI 2011). ISPs (Internet Service Providers) can control communications technically by involving in the network traffic on three levels: network, service or application and subscriber. ISPs can involve in network traffic by regulating e.g. volume and speed. On a level of services and applications, users and contents may be identified or blocked or some applications can be given higher priority than others. Subscribers can be limited e.g. by bandwidth restrictions. Overall, the approach for the control of network traffic management seems to focus on individuals as subscribers and for the utilization of technologies like identity management. (Finnie 2009)

Practically, ISPs can conduct complete monitoring of users activities on the Internet. No other online entity has such panoptical views on users' activity so deeply, because packet sniffs can store everything from e-mail messages to videos and Facebook updates (Ohm 2009).

Practically, intermediaries and service providers can monitor, regulate and control users' connections, use of services and their contents. However, the most extreme conditions are in countries which have build up centralized, state controlled Internet infrastructures, like China. This setting enables three types of restrictions: shutdowns, the deliberate slowing of connection speeds and the imposition of a nationwide system of filtering and surveillance (Kelly & Cook 2011).

Data surveillance and data collection develop forms of indirect censorship as such. Data collection for commercial purposes is very extensive and may be intertwined to the regular uses of Internet. E.g. search for a word like 'depression' on Dictionary.com, may lead to an installation up to 223 tracking cookies and beacons on the users' computer to enable collection of data on a users and further advertising of antidepressants for them.

While practices of data surveillance do not aim at preventing people from expressing their ideas online, they develop unfavorable conditions for the freedom of expression. When the data which users provide, may be stored, accessed and utilized in other contexts later, it may have unexpected impacts or turn for or against users later. (Etzioni 2012)

The most worrying consequence in acceptance of tools of mass control is that citizens get used to it, and questions of the accountability, appropriateness and proportionality of the control mechanisms and the development of the surveillance society become gradually more strenuous. The development of control society is well described in ACLU's "Surveillance Society Clock" (ACLU).

Dimensions of surveillance society are very close already even in Western democracies. A practical example of about this was given in a British television program, Erasing David. A well-known journalist, David, tries to escape the reach of all systems and two private detectives towed him. In one scene, he is on the run somewhere in Europe, and the detectives can show a detailed map of his whereabouts based on his mobile phone data. David succeeded in his escape only for a couple of days. (Erasing… 2010)

4. Criminalization of everyday life

While increasingly sophisticated technologies are used to control citizens, also criminalization of legitimate expression, and adoption of restrictive legislation to justify such measures have been deployed (La Roye 2011). Consequently, the definitions of crime tend to lower and alter, but also sanctions may become stricter (e.g. copyright violations, Hadopi Law).

Citizens juridical position has already practically changed. Citizens may become defined easier as a suspect and even detained in some cases without a valid evidence of a crime if their data indicates some connections. People can be labeled guilty based on the vague evidence of their data - and it is their responsibility to proof that they are innocent (e.g. in case of Hasan Elahi, Elahi 2011). However, this may be an impossible challenge for citizens, if they don't have access on the same data than their prosecutors have. Also, the logic of new practices is completely different from the adopted in juridical practices in many countries according to the Habeas Corpus -principle: citizens are innocent until proven guilty - a fair court trial should precede detention (Habeas Corpus).

At the broadest level, these developments manifest themselves in such models of national level data collection, which previously targeted only for the purpose of criminal investigations like fingerprint and DNA-databases. Countries have swiftly expanded biometric identification methods and implemented or extended databases for the collection of identifying data e.g. fingerprints and DNA (Privacy International 2007).

Same type of lowering criteria concern policies of surveillance (EDRI 2012). People become easier as targets of stricter surveillance, because used criteria of surveillance have not only lowered, but also become vague and versatile. Justifications to stricter surveillance do not need to have links to any crimes, but even peaceful activism and "abnormal behavior" may lead to increased attention (Dziech 2011, Johnston 2009). Especially minorities and marginal groups have already become targets of increasing surveillance (Monahan 2010).

Citizens are treated increasingly as a potential risk for a society, and data surveillance is used to estimate the level of risks they imply (Heinonen 2008). The concept of pre-crime detection reflects extreme interpretation of these ideas by focusing on any "abnormal behavior". Mike Presdee describes these kinds of practices as development as "the creeping criminalization of everyday life" which leads to the "habitualisation and homogenization of everyday life and the disappearance of space" (Boyarsky 2002, Presdee 2000).

The surplus of these developments is a combined use of mass surveillance, lowered level of criminalization and vague concepts of sanctions - and normalizing of these arrangements and extending their focus instead of keeping them as exceptional laws (Saas 2012). These development directions can be recognized even in some Western democracies e.g. in France and USA (e.g. Khaki 2012, Saas 2012). As such, these arrangements legalize permanent monitoring of groups and individuals, which are treated as a risk for a society, by prioritizing risk management over accountability and civil rights (Saas 2012).

5. Ubiquitous information society and extended management of persons and objects

In the ubiquitous environment the control of users extends to the management of persons and objects. The basis for the control is created by comprehensive and more efficient data collection and management procedures which aim at reaching everyone and everywhere. Ubiquitous technologies provide tools to identify, track and monitor any given person or object and their communications and activities. (Karhula 2012b)

Identification is a core element of ubiquitous environment. Identification also means that identifying data is typically linked to all and any other data which is gathered about a certain person in the ubiquitous environment. In this setting, the amount of personalized data, which has a link to personal data, will not only increase, but multiplies and open ups more accurate views on users' data. In addition, all collected data may become permanently stored, searchable, replicable, and accessible, in ways which are beyond their control and to an invisible audience (Hamilton & Moon 2012). (Karhula 2012b)

In ubiquitous environment users become increasingly vulnerable, since there will be more identified data on their communications and activities. Big data has become a concept to indicate the multiplied amounts of data in large data warehouses. Also, ubiquitous data has already become largely as a profitable product, which can be sold for a variety of purposes. In USA for example, at least 52 federal agencies had launched, or were planning to launch at least 199 data mining projects that rely on the services and technology of commercial databases in 2006 (Etzioni 2012). (Karhula 2012b)

Due to the possible long term storage and multipurpose use of the data, person related data may have unexpected and long term impacts for users. Already reviewing ones' Google Account is a shock to many owners of the account. Every search action is stored in its memory, even though it was erased from the personal computer. More than 10 years of Internet history in one online service produces an unreasonably detailed profile of the user.

Automatic analyzes which are largely applied in a processing of ubiquitous data create even more vulnerabilities. Their practices do not forgive or forget the darker occasions during the path of life - they do not have a sense of humor either. Even mistakes or occasional or well-intended humorous information searches or scrolls on sensitive issues can bring about unpleasant surprises by appearing in their profiles, biographies or predictions of their behavior.

In ubiquitous setting person related data has impacts on users by building up suggestions, restrictions or even sanctions for them. It can also have practical consequences, since person related data can control users' access on spaces and services and regulate their activities and communications. Person related data also has wide impacts on social practices; it can define citizens' position and benefits, and practically open or close different kinds of life opportunities for them. As such, ubiquitous environment creates a basis for new kinds of mechanisms of social sorting and discrimination (Lyon 2002). (Karhula 2012b)

6. Database Citizenship - a new form of citizenship

Managing person related information has become a new hot currency and an asset in fighting for the governance of the next phase of the Internet. Google, Facebook, Amazon, eBay and Apple and personal data vendors such as ChoicePoint and Axciom, do massive business on personal data. Rights on the vast amounts of person related data are practically in the hands of data vendors and governments: they own this data, may make profit on it or provide personal data for a basis of decision making. They become kings of personal data economy – but also in the ubiquitous environment as regulators of users' access, communications and everyday activities. (Karhula 2012b)

Database Citizenship is a new form of citizenship, not recognized by the legislator. Information on citizens is stored in numerous databases and registers, which more and more cover also transactional data on users' activities. The extent of collected data partly relates to the person's own activity and role, technical environment and his /her activities on the net. However users' possibilities to regulate data collection are decreasing, since they are increasingly dependent on the networked services and data collection and monitoring practices in networked environment are largely hidden and intertwined to the regular use of the net.

Data Protection Ombudsman Reijo Aarnio prepared a report of all the personal registers and databases in Finland as early as 1988. According to the report, there were already about a million different registers or records (Salminen 2011). The survey lists all the government held public registers and databases like the Population Register, the Land Registry, the Building and Dwelling Register. Municipalities maintain a number of registers related, for example, to health care, education and housing. Registers by banks, credit card companies, payment defaults authorities, trading companies, telecommunication operators and Internet companies are also relevant from the standpoint of ordinary citizens.

Official databases and registers are at least controlled – and in many western countries protected by data protection legislation. In Finland, anyone can demand a registration book on himself/herself. According to law, every register must give a report of its privacy policy. The report should be available for everyone on whom information is collected. (The Office of the Data Protection Ombudsman)

Unfortunately these practices do not concern major global data vendors. Users typically don’t have access on their databases, or have right to manage their data to check its' validity or track uses of their data. Users may not even have control over the data they produce themselves. It may be impossible for them to delete their data and future uses of their data may be uncontrollable. Their data may be merged, manipulated and interpreted outside of the original contexts for various possible purposes. Basically their rights on data may be given contractually to the service provider. Users’ cannot really count on that their data becomes fairly used in a long run, since they don't have means and rights to track or check what kinds of data is stored of them and how it is used. (Karhula 2012b)

All government efforts may not be very transparent either. In USA, it was disclosed in 2006, that three major telecommunications providers, AT&T, Verizon, and BellSouth, had cooperated with the NSA to provide the phone call records of “tens of millions of Americans”— a program which was described “the largest database ever assembled in the world.” (Etzioni 2012)

Feel free to inform us of your national situation.

7. Privatization of the control on the net

Occupation of electronic space is part of expanding network capitalism – and there are constant different kinds of power battles between the major players on the Internet (Manjikian McEvoy 2010). During the Internet period, large international companies, like vendors of network technologies, hardware and software vendors, search engine and social media providers, data vendors and marketing companies have become as major players around networked information. The growing impact of these new stakeholders is also based on the obvious trend of convergence, which has taken place as a fusion of contents, media and networked technologies, but also as a convergence of companies which have merged and consolidated their capacities.

All these parties may regulate access on information, alongside the traditional publishing companies and media. However, the surplus of their controlling capacities goes beyond the dimensions of earlier phases of Internet censorship: these parties may not only involve in contents, but they may control communications and data flows or involve in users activities and communications through data surveillance and their access on person related data. Their wide scale opportunities for surveillance are also taken into account by states; In Europe and USA, governments pressure increasingly internet intermediaries, like ISPs, to directly or indirectly control and monitor network traffic for a variety of reasons from network security to copyright and license violations (EDRI 2011).

A setting of privatized management of contents also provides opportunities to economic censorship. Dominating companies may try to take over the market place, define terms and conditions and functional models for users; or they can impact on users’ rights by defining how much users will be able to manage their data or regulate their data flows. These fears are not philosophical, since e.g. Apple is currently accused of e-book cartel (Whittaker 2012).

The market dominance has also effected on business models like distribution policies. E-journals may be sold in costly packages and there may not be other alternative models available. Availability of articles may be guaranteed only for a certain period and after that already paid issues may be taken away from use (McDermott, 2012). Overall, the price of scientific information has risen steadily, which already threatens researchers', educational institutions' and universities' access to information (Panitch & Machalak 2005, White & Creaser 2007). When access to information is hindered because of the price of the information, high-quality research may diverge into elite universities and colleges, concurrently lowering the quality of education and research at other universities and colleges (Lessig 2011).

Media convergence and concentration of the commerce also put consumers and intermediary organizations, such as libraries, in a less favorable position. Optional contents and bargaining power will diminish. Lawyers of the biggest actors on the market sent smaller individual actors into a corner.

8. Copyright and patent laws narrow access on information

Information flows and the use of information have been recently subjected to regulation especially by means of copyright legislation. Companies use also patents to take over significant means or contents of the virtual space (Gustin 2012).

Copyright restrictions increasingly indicate disproportionate measures in relation to the users like excessively long copyright protection periods, which prevent libraries and museums from digitizing publications and from disseminating them on public networks for everybody to read (McDermott 2012). The most important material of the 20th century is practically speaking commercially copyright protected, although these documents may not be available on bookstores either. Paradoxically, this arrangement does not really bring profits to any party. Also, the lengthy protection period does not comply with the business cycles of publishing and present paradigms of the use of the documents.

At the same time, exemption provisions granted for libraries and museums are getting fewer and fewer. This poses further obstacles to citizens' access to information in the future. Public libraries already struggle hard for the rights of e-book loans (Coffman 2012). Without the right to lend out e-books those libraries are mercilessly marginalized from network developments. Copyright also leads libraries to practical problems without convenient solutions. How the true right holders of the 1930s newspapers can be defined? Why old newspapers cannot be imported freely into the network for a nominal fee?

There has been a move from ownership rights to licenses, which practically means that, the user (e.g. library) can rent or license a publication for its use for a certain period of time (McDermott, 2012). If it needs the publication at some later point, it must be acquired again. These practices develop new kinds of fears. Will the publication even be on the market after 10 years in some readable form? What kinds of contents libraries have after 10 years? This is how we arrive at entirely new questions regarding restricted access to information.

There is a constant battle over virtual space: who owns and regulates it, and who has rights on its' contents and gains profits from it. As Hamilton and Moon indicate, the right time to have influence on these developments is now. Copyright legislation is still under changes, which will indicate if there will be flexibility in the structures of Internet or if the changes will support the old models and interests of industry lobbying (Hamilton & Moon 2012).

9. Intermediaries are called for control

There is an increasing government push for Internet intermediaries, to take a role of controller by investigating, monitoring and sanctioning users. Uses become blocked, logged, monitored, restricted and subjected to sanctions imposed by the intermediaries, who fear legal liability for the actions of their clients. This trend is evident in USA and Europe. (EDRI 2011)

Copyright legislation is among the reasons which are used to set in force these obligations. Direct obligations have been suggested e.g. in ACTA-agreement, French HADOPI law and the UK Digital Economy Act, which require or imply interference with consumers' personal data, blocking of online resources and co-operation with the implementation of sanctions (ACTA, Digital Economy Act, EDRI 2011, Hadopi Law). As such, these arrangements extend forms of surveillance and censorship. They focus on monitoring of all users' data by an excuse of copyright, and at the same time override the borders of users' rights on informational privacy. If these practices become permanent, they may establish structures of control which can be later used for other purposes – and extend the scale of data surveillance and censorship.

Copyright legislation and international agreements have assigned new standards and obligations to organizations which act as intermediaries of networked information to involve in controlling and monitoring of users. These arrangements may also concern parties like hotels, cafes, universities and libraries. (Hamilton & Moon, 2012)

Sanctions of copyright violations have strengthened. E.g. Digital Economy Act in the UK, and the Hadopi law in France apply the so-called three-strike principle (Hadopi Law, Digital Economy Act). If a young member of a family violates the law three times, the access to Internet can be denied from the whole family. If a library offenses the Act three times, it may be disconnected from the Internet. Non-governmental organizations and intermediary organizations, such as libraries, have taken acts to oppose recent decisions to monitor and control citizens' use of information (e.g. in the context of the Digital Economy Act in the UK, and the ACTA-agreement) (Du Preez, 2011, IFLA 2011, IFLA & EBLIDA 2012).

10. Challenging civil rights and democracy

The fundamental right of electronic civil rights is access to information, and free use of information with no threat to privacy. These requirements are no more fulfilled. Censorship and data surveillance have been adopted globally on the Internet. Governments increasingly introduce laws or modify existing laws to extend their power on citizens and monitor Internet users' activities and content of communications without sufficient guarantees for citizens against the abuse of these control mechanisms. (La Rue 2011)

The questions of users' rights and censorship have become more complex: it is no more a question about users' access on information. The control mechanisms on internet may involve in contents, access on contents, communications, distribution, user/distributor or infrastructure by large – and these approaches may combine methods of internet censorship and data surveillance. Availability of Internet access alone, does not guarantee that users have safe environment of communication. Even strictly guarded people in China may have access on the net and availability of local blogs and social media. However, a significant amount of information is filtered out from their availability, and they need to be very careful with their expressions to avoid becoming targets of heavy sanctions.

Overall, the control mechanisms have largely taken over the virtual space without a public discussion about their acceptability, accountability and social effects. At the same time, the broader understanding and public discussion of the dimensions of the control mechanisms and their impact lack behind. Citizens may not be aware of the existence of these control mechanisms or understand the altered definitions of misconduct or crime, since these concepts have become vague.

The developers of the ubiquitous society speak for increasing transparency. This is a fundamental misunderstanding. Ubiquitous environment has so far supported mainly such transparency which is one-directional: users become more transparent for data vendors and managers. However, this does not necessarily work vice versa. Users are more vulnerable for different kinds of misuses of their data and they become targets for tightened control mechanisms. Ubiquitous environment is about extended control and manageability of people and environment, which seems to benefit increasingly data vendors, but they leave users primarily as targets of data collection, tracking and monitoring and provide them limited views and services based on their data. (Karhula 2012b)

Transparency and privacy are among the main concerns when control mechanisms spread around. As such, privacy and transparency complement each other to support the ground rules of constitutional and democratic society. Privacy is crucial for individuals, since other civil rights like freedom of speech, opinion, religion and movement cannot become true without privacy. Informational privacy, which more accurately relates to internet communications, defines limits and protections for individual citizens against the deliberate state involvement into their communications (Bannister, 2005). On the internet, this is a limited picture, since there are also other parties, companies, organizations or individual people, who may override the borders of informational privacy for a variety of reasons. Nonetheless, informational privacy basically includes a right of self-determination and creation of borders in relation to 3rd party involvement into private information and communications.

Openness and transparency of public administration and the exercise of political power are conventionally regarded as signs of high quality of governance and democracy (Firmino, 2010). Accordingly, transparency is a principle which needs to be applied to the government and other organizations which have significant power in a society, to ensure accountability and social acceptability of their actions. This arrangement creates a balancing mechanism for the use of power and control.

The paradox of the present developments of the control mechanisms is that they tend to destroy the basis of civil rights by narrowing down privacy and declining anonymity – but also spread transparency to the wrong direction: towards citizens, when the appropriate use of transparency would be to strengthen the control of powerful actors in society. Now, the safeguards for citizens will erode, while the control mechanisms will increase non-transparency and uncontrollability of the major institutions which hold power – and indeed gives them more power and very efficient tools to manage citizens. (Karhula 2012b)

Erosion of civil rights and democratic principles is an evident consequence, since large-scale control mechanisms and their justifications have often overridden other principles. However, the status of democracy and civil rights are still valid issues of research and public discussion. What is a present state of the quality of democracy? How to find out a healthy balance of powers between citizens, governments and major stakeholders of the Internet? How civil rights could be protected?

Overall, perspectives to the users' rights on the Internet need to extend from contents and access to cover the infrastructure of communications. In this broad context users' should have a right to express versatile views and produce contents which does not reflect the mainstream values without fear. Users should gain more control over the management of their person related data to be able to check, correct and follow up how their person related data is used (e.g. European data protection law recognizes these types of requirements as data subject rights, EDPS 2012).

A closed and non-transparent setting of infrastructural censorship and data surveillance should be opened in a future. Since data collection and management becomes more and more invisible, people need facts about the context in which surveillance schemes are to be deployed (Clarke 2007). In an environment of extended data collection, users would require more protections against tracking, monitoring and use of their data without their consent. Otherwise, the setting of ubiquitous environment may produce fatal consequences for users and society.

Conclusions

Control over Internet contents and communications has extended dramatically, since the beginning of 2000s and it is reflected in technologies, laws and social practices.

The combined effect of these developments is that they have established conditions of large-scale control mechanisms, their juridical justifications and renewed interpretations of civil rights.

Internet censorship and data surveillance may not always produce direct restrictions, but their possible further multipurpose uses of data poses threat for users also in western democracies. In conditions of extensive data collection people are practically pressured into conformity, if they want to protect their benefits and future life opportunities in conditions. In a long run and if these practices become stricter, they may freeze public discussion and develop insecurity and fear in communications. New control mechanisms will threaten the benefits of any minorities or individuals or groups with deviant opinions or life styles in a society. And fundamentally, they concern quality of management and democracy. (Etzioni 2012, Karhula 2012b)

Serious consequences of the opposite direction of the development have been witnessed in totalitarian countries, in which citizens may become heavily sanctioned for any opposing expressions (La Rue 2011). In this respect, the same practices, like forced user identification and data surveillance, which may be justified in certain connections in western democracies, turn life threatening in societies, where the political atmosphere is different.

These same consequences may threaten the relationship between media and citizens, since there are signs of policies, which will threaten the balance of power between citizens and organizations with major power. E.g. protection of sources and users' anonymity in communications within the services of media have been questioned. Journalists are among the target groups of stricter surveillance even in European countries (Privacy International 2011b). Also the tightening competition within media industry inhibits companies to monitoring of their users' communications more thoroughly, which again sets users as targets of data surveillance (Turow 2011).

Protection of sources does not concern only media, but it supports the structures of democracy in society. Whistle-blowing is increasingly recognized as an early warning system and an effective tool for fighting corruption, fraud and mismanagement in society by revealing negligence or wrongdoing. The importance of whistle-blowing has also been confirmed internationally by the UN and OECD (Osterhaus & Fagan 2009). If protection of sources erodes, also a crucial part of such checks and balances of democratic society become destroyed which would ensure acceptability and accountability of the management.

Major players on the Internet have an increasing power on public and private sector.

However, their impact may turn for or against the censoring and surveillance efforts. They could use their significant power by making large scale positive impacts on civil rights and for an open society. Due to the political pressure, consumers' complaints and pressure of activists, companies have also occasionally changed their policies and indicated that they are capable to make ethical choices by request in certain cases. In 2010, Google announced it would stop censoring the Chinese version of its search engine (Fay 2010, Reporters Without Borders 2010). They could also support safer use of internet by providing tools which would improve users' capabilities to protect their privacy and anonymity, or give them more control over their person related data or tracking and locating functionalities: good examples of these anti-censorship measures include Do Not Track –legislation, Net neutrality –efforts, IMMI-project, which aims at gathering the best principles to protect freedom of information as a legislative package (Hastings 2011, Howe & Nissenbaum 2008, IMMI Status report 2012, Pike 2011, Wu 2007).

Censorship is not a new phenomenon. However, internet censorship is more threatening and powerful due to its’ potential global scale and scope. It provides such dimensions of mass media, which are not comparable to earlier settings of censorship (Bitso & Fourie & Bothma 2012). Overall, any efficient and large-scale systems of controls, like ubiquitous environment represents, pose a threat and create significant risks for democratic society and civil rights. Since these comprehensive control systems already have been largely taken into use or their implementation is in progress, it would be necessary to face the conditions and consequences they develop. These developments should be recognized, understood and their social impacts should be estimated. In political decision making, it would be crucial to regulate the tools of mass control and ensure their accountable, acceptable and proportionate use in a way that democracy and civil rights are still valued.

References

- ACLU. Surveillance Society Clock.
- ACTA. Anti-Counterfeiting Trade Agreement.
- Anderson, Nate (2007), US and UK have become "endemic" surveillance societies. ARStechnica.com, 31.12.2007.
- Baloo, Jaya, ETSI & Lawful Interception of IP-traffic. RIPE-48 Meeting, May 2004.
- Bannister, Frank (2005), The panoptic state: Privacy, surveillance and the balance of risk. Information Polity 10 (2005): 65–78.
- BBC News (2010), Timeline: China and net censorship. Last update: 23 March 2010.
- Bitso, Constance & Fourie, Ina & Bothma, Theo (2012), Trends in transition from classical censorship to Internet censorship: selected country overviews. FAIFE Spotlight, 2012.
- Bloss, William (2003), Escalating U.S. Police Surveillance after 9/11: and Examination of Causes and Effects. Surveillance & Society, Part 1, 4(3):2007. p208-228.
- Boyarsky, Nicholas (2002), The Technique of Space. In: Leon Van Schaik & Peter Lyssiotis, Poetics in Architecture: 82-83. London; New York: Architectural Design; WileyAcademy, 2002.
- Carey-Smith, Mark and May, Lauren (2006) The Impact of Information Security
- Technologies Upon Society. In: Proceedings Social Change in the 21st Century. Conference 2006, Queensland University of Technology.
- Clarke, Roger (2007), What is Überveillance? (And What Should Be Done About It?)' IEEE Technology and Society 29, 2 (Summer 2010) 17-25
- Coffman, Steve (2012), The Decline and Fall of the Library Empire. Searcher. April 2012, Vol 20 Issue 3. p14-47. 13p.
- Cohen, Amon (2012), European Parliament Approves U.S. PNR Data Transfer Deal. BusinessTravellerNews.com. 19.4.2012.
- Cross, Tom (2010), Exploiting Lawful Intercept to Wiretap the Internet. Black Hat Technical Security Conference, Jan 2010.
- Deibert, Ron (2012), Cyber Security. In: Evolving Transnational Threats and Border Security. A New Research Agenda. Christian Leuprecht & Todd Hataley & Kim Richard Nossal.(Ed.). Centre for International and Defence Policy, Queens University, Canada.
- Deibert, Ronald J. & Palfrey, John G. & Rohozinski, Rafal & Zittrain, Jonathan (2011), Access contested: Towards the Fourth Phase of Cyberspace Controls. In: Access Contested: Security, Identity and Resistance in Asian cyberspace. Ed. by Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski and Jonathan Zittrain. Cambridge; MIT Press, 2011.
- Digital Economy Act 2010. Wikipedia.
- Du Preez, Derek (2011), Digital Economy Act threatens library internet services. Computing.co.uk, 4.2.2012.
- Dutton, William H. & Dopatka, Anna & Hills, Michael & Law, Ginette & Nash, Victoria (2010), Freedom of Connection – Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet. Oxford Internet Institute, University of Oxford. A report prepared for UNESCO’s Division for Freedom of Expression, Democracy and Peace.
- Dziech, Andrzej (2011). INDECT: Intelligent information system supporting observation, searching and detection for security of citizens in urban environment. Presentation. 10.4.2011.
- EDPS (2012), European Data Protection Supervisor. The data subjects’ rights. Page last modified: 29. heinäkuuta 2012 13:20:35.
- EDRI (2011), The slide from “self-regulation” to corporate censorship. Discussion paper prepared by Joe McNamee.
- EDRI (2012), EU Surveillance: A summary of current EU surveillance and security measures.
- Elahi, Hasan (2011), You Want to Track Me? Here You Go, F.B.I. New York Times, 29.10.2011.
- Erasing David (2010). A documentary about privacy, surveillance and the database state.
- Etzioni, Amitai (2012), The Privacy Merchants: What Is To Be Done? University of Pennsylvania Journal of Constitutional Law 14.4 (March 2012) p. 929-951

- Fay, Joe (2010), Google leaves censorship to China's experts: China crisis not exactly a human rights triumph. The Register. 13.1.2010.
- Finnie, Graham (2009), ISP Traffic Management Technologies: The State of the Art. Heavy Reading. Report for the CRTC.
- Firmino, Sandra (2010), Corruption and quality of democracy. 3rd ECPR Graduate Conference. 30.8.-1.9.2010. Dublin.
- Gindin, Susan E. (1997), Lost and found in cyberspace. Informational Privacy in the age of the Internet.
- Goldberg, Beverly (2012), Patriot Act Renewal Renews Reformers' Determination. American Libraries, 31.5.2012.
- Gschrey, Raul (2011), Borderlines, Surveillance, Identification and Artistic Explorations along European Borders. Surveillance & Society, Vol 9, No 1/2 (2011).
- Gustin, Sam (2012). Patent Wars. Time, 23.4.2012. Vol. 179 Issue 16.
- Habeas corpus. Wikipedia.
- Hadopi law. Wikipedia.
- Hamilton, Stuart & Moon, Darren (2012), The Struggle to Scale: Keeping Up With the Internet. FAIFE Spotlight, 2012.
- Hastings, Peter (2011), "Do not track or right on track? – The privacy implications of online behavioural advertising". Public Lecture, University of Edinburgh, School of Law. Edinburgh, 7.7.2011. AHRC/SCRIPT and BILETA Policy Forum, 7-8.7.2011, University of Edinburgh, John McIntyre Conference Centre.
- Heinonen, Risto (2008), There is no privacy in the everyday information society. In: Paratiisi vai panoptikon? - näkökulmia ubiikkiyhteiskuntaan. Päivikki Karhula (toim.). 2008. 192 s.
- Howe, Daniel C. & Nissenbaum, Helen (2008), Track me not: resisting surveillance. In: Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society. Kerr, Ian & Steeves, Valerie & Lucock, Carole (ed.). Oxford: Oxford University Press (2008).
- IFLA (2011), IFLA Statement on Intermediary Liability for the IGF. Internet Governance Forum (IGF), Nairobi, Kenya
- IFLA & EBLIDA (2012), IFLA and EBLIDA Statement on ACTA and the Importance of Multilateral Multi-stakeholder IP Policy Formation. The Hague, 2 July 2012.
- IMMI Status Report (2012). April 2012.
- Johnston, Ian (2009), EU funding 'Orwellian' artificial intelligence plan to monitor public for "abnormal behaviour". The Telegraph, 19.9.2009.
- Karhula, Päivikki (2012a), Data driven futures. FAIFE Spotlight, 5.6.2012.
- Karhula, Päivikki (2012b), Information and communication related control in a ubiquitous environment. (Unpublished article)
- Kelly, Sanja & Cook, Sarah (2011), New technologies, innovative repression: Growing Threats to Internet Freedom. In: Freedom on the Net 2011: A Global Assessment of Internet and Digital Media. Freedom House.
- Khaki, Ateqah (2012), Indefinite Detention is Un-American. ACLU Blog of rights. 6.6.2012.
- La Rue, Frank (2011), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. United Nations. Human Rights Council. 16 May 2011. Seventeenth session, Agenda item 3. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development.
- Lessig, Lawrence (2011), The Architecture of Access to Scientific Knowledge. Lecture at CERN, Geneva, Switzerland, 18 April 2011.
- Lyon, David (2002), Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination. London : Routledge, 2002.
- McDermott, Abigail J. (2012), Copyright: Regulation Out of Line with Our Digital Reality? Information Technology & Libraries. March, 2012, Vol. 31 Issue 1, p7-20. 14p.

- Manjikian McEvoy, Mary (2010), From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. International Studies Quarterly (2010) 54, 381–401.
- Monahan, Torin (2010), Surveillance in the Time of Insecurity. Rutgers university press, New Brunswick, New Jersey, and London.
- Morozov, Evgeny (2011), The net delusion: the dark side of Internet freedom. New York, NY : PublicAffairs, 2011.
- The Office of the Data Protection Ombudsman. Data protection in Finland
- Mueller, Milton (2010). Security Governance on the Internet. In: Networks and states: The Global Politics of Internet Governance, 280. MIT Press.
- O'Brien, Mark (2010), Law, privacy and information technology: a sleepwalk through the surveillance society? Information & Communications Technology Law. Vol. 17, No. 1, March 2008.
- Ohm, Paul (2009), The Rise and Fall of Invasive ISP Surveillance. University of Illinois Law Review, 2009 (5): 1417.
- Osterhaus, Anja & Fagan, Craig (2009), Alternative to silence: Whistleblower protection in 10 European countries. Transparency international, 2009.
- Panitch, Judith M. & Machalak, Sarah (2005), The serials crisis. A White Paper for the UNC-Chalep Hill Scholarly Communications Convocation. Janury, 2005.
- Pike, George H. (2011), What the Future Holds for Net Neutrality. Information Today, June 2010, Vol. 27 Issue 6.
- Presdee, Mike (2000), Cultural Criminology and the Carnival of Crime. London; New York: Routledge, 2000.
- Privacy International (2004), Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection. Privacy International in co-operation with European Digital Rights Initiative, the Foundation for Information Policy Research, and Statewatch. February, 2004.
- Privacy International (2007), The 2007 International Privacy Ranking. Leading surveillance societies in the EU and the World 2007. 28.12.2007. Privacy International.
- Privacy International (2011a), Our response to the EU consultation on legality of exporting surveillance and censorship technology. 31.10.2011.
- Privacy International (2011b), Surveillance Monitor 2011: Assessment of surveillance across Europe. 26.1.2011.
- Reporters Without Borders (2011), Internet Enemies. 12 March 2011.
- Reporters Without Borders (2012), Beset by online surveillance and content filtering, netizens fight on. 13.3.2012.
- Salminen, Juho (2011), Suomessa miljoona henkilörekisteriä. Isoilta ruumiilta vältytty. Suomen kuvalehti, 9.11.2011.y
- Saas, Claire (2012), Exceptional Law in Europe with Emphasis on "Enemies". Draft. Conference presentation in: Preventive Detention and Criminal Justice, Ravenna, May 11 – 12, 2012.
- Turow, Joseph (2011), The Daily You. Yale University Press, 2011.
- Waugh, Rob (2012). New surveillance cameras will use computer eyes to find 'pre crimes' by detecting suspicious behaviour and calling for guards. Daily Mail Online. Published, 5.6.2012 13:12 GMT, Updated 5.6.2012 13:12 GMT.
- White, Sonya & Creaser, Claire (2007), Trends in Scholarly Journal Prices. March 2007. Loughborough, LISU, 2007.
- Whittaker, Zack (2012), DoJ sues Apple, publishers in e-book price fixing antitrust suit. ZDNet, 11.4.2012.
- Wu, Tim (2007), Network Neutrality FAQ. Last modified: 25.8.2007.