ISSN 2029-1701

Mokslinių straipsnių rinkinys
VISUOMENĖS SAUGUMAS IR VIEŠOJI TVARKA
PUBLIC SECURITY AND PUBLIC ORDER
2011 (6) Scientific articles

THE LIMITING OF PRIVACY IN THE CYBERSPACE

Birutė Pranevičienė [1]

[1] *Mykolas Romeris University, Faculty of Public Security, Department of Law*
Putvinskio g. 70, LT-44211 Kaunas
Telefonas 303655
El.paštas: praneviciene@mruni.lt

Darius Amilevičius[2]

[2]*Mykolas Romeris University, Faculty of Public Security, Department of Humanities*
Putvinskio g. 70, LT-44211 Kaunas
Telefonas 303664
El.paštas: d.amilevicius@mruni.eu

Summary. The numbers of internet users are growing rapidly. A recent innovation is the creation of virtual worlds which promise an entire social life in cyberspace. During last decades information technology is considered as a major threat to privacy, because it makes prerequisite of pervasive surveillance, large databases, and lightning-speed distribution of information across the world. There are continual limitings of privacy and personal data abuse, made by Internet services providers. After the attacks of terrorist of September 11, 2001 in New York, communities around the world revalued existing rules and methods of dealing with information. The limiting of privacy is settled by law enforcement and by governments. The main question arise: does the privacy in its classical meaning match to the actual state of things?

Keywords: Cyberspace, Human Rights, Privacy, Security.

INTRODUCTION

During past two decades human life has extremely changed. As Michael Specter noticed, „There are now more than a billion pages on the World Wide Web, all loosely tied together by seven billion annotated links [...] which is at least one link for every person on the planet. Each day, more than a million pages are added [...] For the first time in history, people everywhere have access to the thoughts, products, and writing of a large – and growing – percentage of the earth‘s population”.[1] Together with growing World Wide Web, the huge growth in e-mail, blogs, message boards and messenger services has intervened during last years. A recent innovation is the creation of virtual worlds which promise an entire social life in cyberspace. „Almost two-thirds of all adults now log on to the web. We spend more and more of our time staring at computer screens“[2].It is impossible not to use internet in present days, and the number of internet users is growing rapidly. For example, at the recent F8

[1] Specter, M. *Postcard from Silicon Valley*. The New Yorker, Spring 2000.
[2] Easton, M. *Does happiness live in cyberspace*?. In *BBC News* [interactive] [accessed 2011-10-01] <http://news.bbc.co.uk/2/hi/programmes/happiness_formula/5052078.stm>

conference Facebook revealed that they have 800 million active users now. Europe, with Russia included, has a population of 727 million. Consequently, there is a social network so large that it could fill up a major world region with people. Another remarkable comparison is that Facebook now has as many users as the entire Internet did back in 2004, the year Facebook was founded[3].

No matter where we spent our time – at home, in workplace, in public space or in cyberspace, we have a right to expect inalienability of our fundamental rights, such as freedom of thought, protected dignity, right to privacy, etc. During last decades information technology is considered as a major threat to privacy, because it makes prerequisite of pervasive surveillance, large databases, and lightning-speed distribution of information across the world. People go and drive somewhere, they buy something, they apply for a job, they pay their bills, they write emails, communicate with others and etc., in other words - people live and at each of those moments of their life, their personal information is collected, retained and processed. The extent of radical transformations of the technology have created the remarkable range of present-day systems, including distributed networking, the World Wide Web, mobile devices, video, audio, and biometric surveillance, global positioning, ubiquitous computing, social networks, sensor networks, databases of compiled information, data mining and more. A set of worries about privacy is associated with each of these developments. [4] Therefore, it makes sense to ask the question: what can we reasonably expect seeking to keep private?

The aim of this article is to disclose emerging threats for privacy, caused by using information technologies and to present the arguments dissenting from legitimate interest of an individual to the privacy in cyberspace.

Objectives of the Research. 1. To disclose the threats to privacy on the internet. 2. To justify the limiting of privacy by legal regulation. 3. To reconsider how much the privacy in its classical meaning maches the actual state of things on the internet.

Methodology of the Research. In the course of reaching the objective of the research were used the methods of systemic, analytical-critical, and documentary analysis.

[3] Data sources [accessed 2011-10-01]: <http://www.facebook.com/pingdom/posts/123197607785796, http://www.internetworldstats.com/, http://www.geohive.com/earth/pop_region.aspx>.
[4] Nissenbaum, H. *Privacy in Context California*. Stanford: Stanford University Press, 2010, p.1-51.

1. THREATS TO PRIVACY ON THE INTERNET

According to Alan Westin, „Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others“[5]. Numerous other scholars have presented similar theories: „The essence of privacy is no more and certainly no less, than the freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behaviors and opinions are to be shared with or withheld from others“[6]; „We built our own definition of privacy on what we consider the most elegant definition, „informational self-determination“, which refers to a person‘s ability to control the flow of his own personal information“[7]; „Freedom of private life – is a universally useful recognition, that there is a space for existence, that belongs solely to the individual and others may not be permitted to trespass it.“[8].

Automated data processing option poses a serious threat to privacy, because it can be moved from one location to another and these operations are not expensive and does not affect the amount of time. States created a variety of registers, which collect personal data. State records contain information relevant to different groups in society. The information is necessary for authorities for the performance of government functions, such as social welfare, tax administration and others. Information, containing residents and business records, allows individuals to protect property rights. Business records information necessary to evaluate the creditworthiness of customers, proactively protect themselves against insolvent customers or to recover the debt, as well as carrying out market studies and marketing campaigns. Therefore, possibility to collect data, to keep it, to harmonize and to use this information became very easy by informational technologies. There are large databases and Internet records of information about individual financial and credit history, medical records, purchases and telephone calls, etc. and most people do not know what information is kept about them or who has access to it. The possibility for others to access and link the databases, almost without control of using or sharing the information, makes individual control over information oneself more difficult than ever before.

[5] Westin, A. *Privacy and Freedom*. New York, Atheneum, 1967, p.7.
[6] Ruebhausen, O.M. and Brim, O.G. *Privacy and Behavioral Research*. Columbia Law Review, 1965, p. 1184.
[7] Goldberg, I., Hill, A., Shostack, A. *Trust, Ethics and Privacy*. Boston University Law Review, 2001, p. 407.
[8] *Lietuvos Respublikos konstitucijos komentaras* [Commentary of the Constitution of Lithuanian Republic], ed. Jovaišas, K. Vilnius, Teisės institutas, 2000, P. 163.

Networking technologies to exchange personal data has become very fast, low cost and high quality. People are incredibly at risk as technology improves Let us bring some examples.

First of all, let us bring a brief consideration what is "cookie" and how it works. A "cookie" is a piece of information that an Internet website sends to surfer's browser when he access information at some site. Upon receipt of the information surfer's browser saves the information on a hard-disk (unless a browser doesn't support "cookies"). Each time surfer uses his computer to access the same website, the information that was previously received is sent back to the website by user's browser. Most commonly used browsers support the use of "cookies". Why are "cookies" used? Generally, for those of surfers who access the Internet through public Internet service providers, each request surfer makes to a website cannot be linked to a previous request, as each request does not contain a permanent unique identifier. "Cookies" allow website operators to assign a unique permanent identifier to a computer which can be used to associate the requests made to the website from that computer. "Cookies" indicate to a website that some surfer has been there before and can be used to record what parts of a website he visits. While "cookies" themselves may not identify surfer, in the way a name or address does, a "cookie" could potentially be linked with other identifying information. For example, if a surfer provides extra information about himself to a website by buying something on-line or subscribing to a free service, then the "cookies" can be used to build up a profile of buying habits and interests of a surfer. Later this information can be used advertising surfer's interests. Many web surfers object strongly to "cookies" as they feel that "cookies" invade their hard drive without permission.[9]

Google Inc. is a first and foremost data company. Google of a past had a concept of "do no harm"; the new concept now is "I want control". In the past, it competed by manipulating publicly available data better than its competitors. By doing this, it had unprecedented success. Since everyone has reasonably equal access to the internet's content, leaders have been striving to gain access to private data. The most cost effective way of doing this for the engines is by collecting data from the users that already use their services. Google has been increasingly serving its users by using their personal data to manipulate public data in individualized ways. Some methods are:

[9] Penenberg, A. Cookie Monsters In *Slate* [interactive] 2005 Nov. 7. [accessed 2011-10-01]. <http://www.slate.com/articles/technology/technology/2005/11/cookie_monsters.html>.

1. Click Tracking – Google logs all the navigational clicks (ads, actions, feature clicks, etc) of all of its users on all of its services.

2. Forms – Along with the data the user enters directly into the forms (username, password, etc), Google logs the time and date and location of submission

3. Cookies – Google uses cookies on all of its web properties. Additionally, it leaves advertising (Doubleclick) cookies to track users' movement around the web. By doing this, Google can track individual users on any page that has either Doubleclick or Adsense ads. This means millions of pages that are not on Google's web properties.

4. Server Requests Stored in Log Files – Every request made to any of Google's server is stored in log files. The content stored is dependent on the type of request.

5. Store – Google uses an internal database called BigTable spread over approximately one million servers[10]. That puts Google's disclosed data size at over 1 Petabyte (1,048,576 GB). This doesn't even consider AdSense, Gmail, Google Maps, Street View, Google Images, or other private databases.

One can ask: what specific user's data Google collects? Below is a list of some *self-declared* piece of datum that Google collects when a user interacts with its many web services. This means there is even more user's data that is gathered by Google, but is known to the public.

Google (normal search): search engine result pages; country code domain; query; IP address; number of results; additional preferences can include street address, city, state, zip/postal code; server log (query, URL, IP address, cookie, browser, date, time); clicks.

Google (personalized search): logs every website visited as a result of a Google search; content analysis of visited Websites.

Google Account: used as resource to compile information on individual users; sign up (sign up date; username; password; alternate E-mail; country); personal picture; usage (friends; Google services usage; amount of logins).

Gmail: Stores, Processes and Maintains all messages; Account Activity; Data displayed; Links clicked; Stores all e-mails; Contact Lists; Spam trends; Gchat (All conversations and who they involve; When service is used); Size of contact list; Contacts communicated with; Frequency of data transfers etc.); Size of data transfers; Clicks.

[10] Chang, F., Dean, J., Ghemawat, S., and oths. *Bigtable: A Distributed Storage System for Structured Data.* Google Inc. Research informations [interactive]. 2006, [accessed 2011-10-01]. <http://labs.google.com/papers/bigtable-osdi06.pdf >.

Google Checkout: buyers (full legal name; credit card number; debit card number; card expiration date; card verification number; billing address; phone number; e-mail address; sellers; bank account number; personal address; business category; government-issued identification number; social security number; taxpayer identification number; sales volume ecc.).

YouTube: YouTube SERP data; registered user data; videos uploaded; comments posted; videos flagged; subscriptions (contacts; all videos watched; frequency of data transfers; size of data transfers; click location data; information display data); e-mail; account basics (e-mail, password, username, location (country), postal code, birth date, gender).

Picasa: friend graph; favorite lists; clicks (almost all Google services track all clicks); all photos; Geotags; people who subscribe to albums.[11]

There are many different aspects of Google's data collection. The IP addresses from which the client application is logging in, cookies are used for settings and tracking purposes, and if surfer is logged into his Google account, what he does on Google-owned sites can often be coupled to him personally, not just his computer. In short, if surfer uses Google services, Google will know what he is searching for, what websites he visits, what news and blog posts he read, and more. As Google adds more services and its presence gets increasingly widespread, the so-called *Googlization* of almost everything continues. It's impossible to use the Internet without touching a single one of Google's services (without YouTube, Twitter, Gmail, Google search etc.).

With all this information at its fingertips, Google can group data together in very useful ways. Not just per user or visitor, but Google can also examine trends and behaviors for entire cities or countries. It should be mentioned that Google's isn't alone in doing this kind of data collection. Microsoft is doing similar things with Bing and Hotmail, to name just one example. If Google can make that much data publicly available, we can just imagine the amount of data and the level of detail Google can get access to internally.

Nowadays a smartphone became the most dangerous possession. So much of surfers screen time is shifting from Personal Computers to smartphones. The amount of personal information on that phone is very huge – it's like carrying a mini-computer around with us. Now smartphones double wallets and bank accounts - allowing users to manage their finances, transfer money, make payments, deposit checks and swipe their phones as credit

[11] Dover, D. *The Comprehensive List of All the Data Google Admits to Collecting from Users.* Seomoz,, 2008 [accessed 2011-10-01]. <http://static.seomoz.org/user_files/google-user-data/SEOmoz-Google-User-Data.pdf>.

cards - they are very lucrative scores for thieves. And with 30% of phone subscribers owning iPhones, BlackBerrys and others, there are a lot of people at risk.

Attacks on smartphones climbed to an all-time high in 2010. Specifically, attacks on Google's Android smartphones quadrupled, and smartphones running Java-based applications jumped 45% [12]. On the other hand, Apple isn't alone in tracking the location of its iPhone customers - it turns out, that if one uses an Android phone, Google is keeping an eye on him, too.

The information, that the iPhone secretly tracks its users' location data, came to light in 2011, and it set off a firestorm of privacy-related controversy from security experts and academic researchers. Initially, experts said the data was stored only on the iPhone and Apple didn't collect it. But Apple does collect the location logs. And Apple is not alone: Google receives location data about its phone users at least several times an hour. Android phones transmit to Google the names, locations and signal strengths of nearby Wi-Fi networks.[13]

Citing the research firm Gartner, Inc., the Wall Street Journal wrote that Google and Apple are tracking their phone users' location data to tap the $2.9 billion market for location-based services that expected to rise to $8.3 billion in 2014"[14].

Location-based services allow companies to more specifically target customers by region, and can help advertisers and marketers hit you with specific ads based on where you live. Google has previously said it uses location logs to help compile databases of Internet Wi-Fi hotspots, which can help cell networks better route calls and build traffic maps. This is not the first time Google has come under fire keeping close tabs on its users.

The fact is that databases like Google Streetview's Mac-to-Location database or the Skyhook[15] database can be used to direct attackers to a person's home. It just underlines how much responsibility companies that collect such data have to safeguard it correctly.[16]

[12] *Global Security insight for Mobile Report* [interactive]. AdaptiveMobile, 2011 [accessed 2011-10-01]. <http://www.adaptivemobile.com/global-security-insight-centre>.

[13] Liebowitz, M. Google's Android Phones Track You Just Like iPhones. In *Security News Daily* [interactive] Apr 22, 2011 [accessed 2011-10-01]. <http://www.securitynewsdaily.com/googles-android-phones-track-you-just-like-iphones-0720/>.

[14] Angwin, J., Valentino-Devries, J. Apple, Google Collect User Data. In *The Wall Street Journal* [interantive] April 22, 2011 [accessed 1011-10-01].
<http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html>.

[15] Skyhook's Core Engine is a software-only location system that quickly determines device location with 10 to 20 meter accuracy.

[16] Web attack knows where you live. In *BBC News Technology* [interactive]. August 3, 2010 [accessed 2010-10-01]. <http://www.bbc.co.uk/news/technology-10850875>.

Information is very valuable. In this century it's impossible to stay off internet. And avoiding Google is not the correct solution either. If not Google someone else will collect the data. This is the trend we are heading to. But all people are entitled to know in details what is going on with their personal data. Are the laws regulating internet strong enough to stop someone from abusing with the data they have at hand? Are people entitled for private space?

2. JUSTIFICATION OF THE LIMITING OF PRIVACY BY LEGAL REGULATION

The right to privacy is not an absolute right, in other words, societies can determine the grounds of its limitation. Thus government can decide and issue laws which limit right to privacy in some ways. There are competing interests in societies: for example, in some countries individual privacy may conflict with freedom of speech laws and some laws may require public disclosure of information which would be considered as private in other countries and cultures. Equally important in understanding of the legal right to privacy is an understanding of other interests that may override it. Whenever an invasion of privacy is claimed, there are usually competing values at stake. Different legal doctrines govern the resolution of a given conflict, depending on the area of privacy involved.

Increasing concern about crime and terrorism, and calls for stricter law enforcement, have led to measures expanding the authority of police to enter our homes, search our belongings, and intercept our communications. And the notion that information can be kept secret to any degree may simply vanish in cyberspace.

International documents devoted to protection of human rights embedded particular human rights and simultaneously determined the limits of those rights. The most important and historically significant international document is the Universal Declaration of Human Rights, adopted by the United Nations in 1948. Article 12 of the Declaration states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[17] Article 29 of the Declaration states: "In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the

[17] The Universal Declaration of Human Rights, Article 12 [2011-09-20] <http://www.un.org/en/documents/udhr>.

rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society."[18]

European Convention for the Protection of Human Rights and Fundamental Freedoms, adopted by the Council of Europe in 1953, also enshrines right to respect for private and family life:" Everyone has the right to respect for his private and family life, his home and his correspondence." [19] This right involves not just preventing intimate acts or one's body from being seen by others, preventing unwelcome searching of one's personal possessions, preventing unauthorized access to one's home, but also it involves protection from all possible invasions to our privacy, it means – secures privacy in cyberspace as well. However, Article 8 part 2 of the Convention states: „There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others."[20]

Lithuanian Constitution's provisions, related with the right to privacy, are constructed similarly: Article 22 part 1, 2 and 4 enshrines right to privacy: "The private life of a human being shall be inviolable. Personal correspondence, telephone conversations, telegraph messages, and other communications shall be inviolable […] The law and the court shall protect everyone from arbitrary or unlawful interference in his private and family life, from encroachment upon his honour and dignity".[21] However, part 3 of the Article 22 foresees exceptions from the right to privacy: "Information concerning the private life of a person may be collected only upon a justified court decision and only in accordance with the law."[22]

Thus, these main documents, which are legally binding in Lithuania, embedded right to privacy, and at the same time fixed the grounds of privacy's limits. The main arguments, allowing the legalization of the right to privacy restrictions, are tied to the interests of:

1) national security,
2) public safety,
3) economic well-being,

[18] The Universal Declaration of Human Rights, Article 29 [2011-09-20] <http://www.un.org/en/documents/udhr>.
[19] Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8 part 1 [2011-09-22] <http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/ENG_CONV.pdf>.
[20] Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8 part 2 [2011-09-22] <http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/ENG_CONV.pdf>.
[21] Constitution of the Republic of Lithuania, Official Gazette, 1992, No. 33-1014, Article 22, parts 1,2 and 4.
[22] Constitution of the Republic of Lithuania, Official Gazette, 1992, No. 33-1014, Article 22, part 3.

4) protection of health or morals;
5) protection of the rights and freedom of others;
6) prevention of disorder or crime.

Even if there appears danger to above mentioned values, intervention to somebody's privacy could be made in accordance with the law. The second important thing is, that the law, limiting right to privacy, should be necessary in a democratic society. In other words, legislative cannot act arbitrarily and to pass the law, which abridges the right to privacy, without identification whether the threats to national security or public safety are real, or hypothetical.

National and human security is extremely important in human society, because it is one of the biggest needs of human being. According to Maslow pyramid, safety is the main need of human beings, while self – actualization is on the top of this pyramid. In the 21st century the style of war has extremely changed. Cyber technologies allow make bigger harm than simple guns. This includes cyber wars, riots, and thefts.

As Amitai Etzioni said: "Before limiting privacy, a well-balanced, communitarian society first determines how well documented various reported dangers to the common good are and how encompassing their expected consequences will be. When many thousands of lives are lost and many millions more are at risk, as with HIV, we face a clear and major threat. The effects of abusing marijuana are real but of a much lower magnitude, and hence do not justify the same kind of response."[23] The same "clear and major threat" standard should apply for limiting privacy in cyberspace.

After the attacks of terrorist of September 11, 2001 in New York, communities around the world revalued existing rules and methods of dealing with information. Thus, in 2002 European Parliament issued the Privacy and Electronic Communications Directive[24], which embedded not only to respect the fundamental rights in the context of processing personal data relating to the delivery of communications services, but also it deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies. The Directive also regulates data retention issue, and under the Directive, Member States may withdraw the protection of data only to allow criminal investigations or to safeguard national security, defense and public security. In order to ensure

[23] Etzioni, A., *The Limits of Privacy*. New York: Basic Books, 2000, p. 14.
[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2011-09-28] < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF>.

the availability of communication data for the purpose of investigation, detection and prosecution of criminal offences, the Directive established provisions for the retention of data. Under the terms of the Directive, Member states of European Union passed laws mandating the retention of the traffic and location data of all communications taking place over mobile phones, SMS, landline telephones, faxes, e-mails, chatrooms, the Internet, or any other electronic communication device.

Later on, in 2006, the so called Directive on Mandatory Retention of Communications Traffic Data[25] was adopted. Preconditions for this Directive was the Conclusions of the Justice and Home Affairs Council of 19 December 2002 which underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications is particularly important and therefore a valuable tool in prevention, investigation, detection and prosecution of criminal offences, in particular organized crime. Also "The Declaration on Combating Terrorism, adopted by the European Council on 25 March 2004, instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers."[26]

Thus, Directive on Mandatory Retention of Communications Traffic Data requires Member States to demand providers of communications to retain communications data for a period of between 6 months and 2 years.

"Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, *inter alia*, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organized crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an

[25] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [2011-10-01] < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>.
[26] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [2011-10-01] < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>.

instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure."[27]

"Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive."[28]

„This Directive aims to harmonize Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network."[29]

3. THE LIMIT OF PRIVACY OR THE DEATH OF PRIVACY IN ITS CLASSICAL MEANING?

Charles Nevin writes: "This is an age which happily invades its own privacy"[30].

On the one hand, we have Universal Declaration of Human Rights, European Convention for the Protection of Human Rights and Fundamental Freedoms, Human rights doctrine etc., that protect Human Right to privacy in its classical meaning. And we have legal attitude that put some limits on it.

[27] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [2011-10-01] < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>.

[28] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [2011-10-01] < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>.

[29] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks Article 1 [2011-10-01] < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>

[30] Nevin, Ch. Taking liberties. In *The Economist:* Intelligent Life Magazine [interactive]. Summer 2009 [accessed 2011-10-01]. <http://moreintelligentlife.com/content/charles-nevin/taking-liberties>.

On the other hand, after the attacks of terrorist of September 11, 2001 in New York, communities around the world revalued existing rules and methods of dealing with information, because national and human security is extremely important in human society. This has brought us to the privacy paradigm shift.

In 2001, Sun Microsystems Inc. CEO Scott McNealy at the Gartner Symposium/ITxpo 2001 have declared that privacy is dead and predicted that the attacks will usher in greater attention to security technology. In turn, privacy will suffer even more than it already has at the hands of technology[31]. In 2006, very famous privacy expert Steven Rambam [32] during his presentation at the Stevens Institute in Hoboken has announced his main thesis: "Privacy is dead! Get over it!". In his presentation, S. Rambam gives deep insight into the possibilities of privacy invasion through tools that are freely available on the internet. He gives examples of Myspace, Facebook, blogs, etc., and also shows how companies like Google or even Domino's Pizza are using data-mining to get a profile of their customers[33]. In 2010, Internet security expert S. Kamkar (about his experiment see in this article above) during his presentation at the Black Hat conference said: "Privacy is dead, people. I'm sorry".[34]

In 2010, Paul Chambers was arrested in United Kingdom under terrorism provisions after making an ill-advised joke on the social networking web site Twitter. As Jason Walsh said: "<…> should jokes be something that we consider ill-advised? <...> Mr Chambers made a remark that many of us might make in everyday conversation: he joked that he would bomb an airport if it didn't re-open in time for his flight <...> It is the unfortunate reality that such jokes are not viewed with levity in potential terrorist targets such as airports and train stations – as former ministry of justice employee George McFaul found out to his cost after being sentenced to twelve months in prison for making smartalec remarks on the Tube in 2008. Questions of public safety in crowded places are one thing, but is it really the case that making an off-hand remark on the internet is cause for an official investigation? Despite the

[31] Hamblen, M. McNealy calls for smart cards to help security. In *Computerworld* [interactive]. October 21, 2001 [accessed 2011-10-01]. <http://www.computerworld.com/s/article/64729/McNealy_calls_for_smart_cards_to_help_security>.

[32] Steven Rambam has coordinated investigations in more than fifty countries, and in nearly every U.S. State and Canadian province. Steven specializes in international and multi-jurisdictional investigations, and within the past few years he has conducted investigations in Israel, South Africa, Holland, France, England, India, Mexico, Guatemala, Spain, Portugal, Bulgaria, Germany, Abu Dhabi, China, Mongolia, the Philippines, Thailand, Laos, Jordan, Vietnam and Brazil, among other locations

[33] Rambam, S. Privacy is dead! Get over it! In *Loss of Privacy* [interactive]. November 28, 2010 [accessed 2011-10-01]. <http://www.lossofprivacy.com/index.php/2010/11/steve-rambam-privacy-is-dead-get-over-it/>.

[34] Web attack knows where you live. In *BBC News Technology* [interactive]. August 3, 2010 [accessed 2010-10-01]. <http://www.bbc.co.uk/news/technology-10850875>.

staggering incompetence of alleged underpants bomber Umar Farouk Abdulmutallab, I have yet to hear of any terrorist quite stupid enough to announce his or her plans days in advance in an open forum such as Twitter <...> Besides, in the immortal worlds of the late bomb jokes may be forbidden at airports, but who decides what's acceptable?"[35].

The societies are worrying about their security. The young generation has different comprehension of privacy that requires more attention of academical researchers. In some way, the legal limitation of privacy goes in hand with the abuse of privacy by Internet services providers for their commercial purposes.

It could be that leaving industrial era and entering in the information era, the concept of "privacy" must be reviewed and actually we are facing the privacy paradigm shift.

CONCLUSIONS

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others. Freedom of private life – is a universally useful recognition, that there is a space for existence, that belongs solely to the individual and others may not be permitted to trespass it. Nowadays the Human Right for privacy in internet is limited. The abuse of internet surfers' privacy is growing continually. There are no laws regulating internet strong enough to stop Internet services providers from abusing it.

The right to privacy is not an absolute right, in other words, societies can determine the grounds of its limitation. Thus government can decide and issue laws which limit right to privacy in some ways. Whenever an invasion of privacy is claimed, there are usually competing values at stake. Different legal doctrines govern the resolution of a given conflict, depending on the area of privacy involved. Increasing concern about crime and terrorism calls for stricter law enforcement. After the attacks of terrorist of September 11, 2001 in New York, communities around the world revalued existing rules and methods of dealing with information. Governs have settled legal limits on privacy.

The societies are worrying about their security. The young generation has different comprehension of privacy that requires more attention of academical researchers. In some way, the legal limitation of privacy goes in hand with the abuse of privacy by Internet

[35] Walsh, J. *Paul Chambers: "privacy is dead, get over it" is not good enough*. In *Globalcomment* [interactive]. January 19, 2010 [accessed 2011-10-01]. <http://globalcomment.com/2010/paul-chambers-privacy-is-dead-get-over-it-is-not-good-enough/>.

services providers for their commercial purposes. It could be that leaving industrial era and entering in the information era, the concept of "privacy" must be reviewed, and actually we are facing the privacy paradigm shift.

REFERENCES

1. Constitution of the Republic of Lithuania, Official Gazette, 1992, No. 33-1014, Article 22, part 3.
2. The Universal Declaration of Human Rights, Article 12 [accessed 2011-09-20] <http://www.un.org/en/documents/udhr>.
3. The Universal Declaration of Human Rights, Article 29 [accessed 2011-09-20] <http://www.un.org/en/documents/udhr>.
4. Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8 part 1 [accessed 2011-09-22] <http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/ENG_CONV.pdf>.
5. Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8 part 2 [accessed 2011-09-22] <http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/ENG_CONV.pdf>.
6. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [accessed 2011-09-28] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF>.
7. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [accessed 2011-10-01] <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>.
8. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [accessed 2011-10-01]. < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>.
9. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [accessed 2011-10-01] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>.
10. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [accessed 2011-10-01] < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>.
11. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks Article 1 [2011-10-01] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.
12. *Lietuvos Respublikos konstitucijos komentaras* [Commentary of the Constitution of Lithuanian Republic], ed. Jovaišas, K. Vilnius, Teisės institutas, 2000.
13. Angwin, J., Valentino-Devries, J. *Apple, Google Collect User Data*. In *The Wall Street Journal* [interantive] April 22, 2011 [accessed 1011-10-01]. <http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html>.

14. Chang, F., Dean, J., Ghemawat, S., and oths. *Bigtable: A Distributed Storage System for Structured Data* [interactive]. Google Inc.: Research informations, 2006 [accessed 2011-10-01]. <http://labs.google.com/papers/bigtable-osdi06.pdf >.
15. Dover, D. *The Comprehensive List of All the Data Google Admits to Collecting from Users* [interactive]. Seomoz, 2008 [accessed 2011-10-01]. <http://static.seomoz.org/user_files/google-user-data/SEOmoz-Google-User-Data.pdf>.
16. Easton, M. *Does happiness live in cyberspace*? [interactive]. *BBC News, 7 June 2006* [accessed 2011-10-01]. <http://news.bbc.co.uk/2/hi/programmes/happiness_formula/5052078.stm>.
17. Etzioni, A. *The Limits of Privacy*. New York: Basic Books, 2000.
18. *Global Security insight for Mobile Report* [interactive]. AdaptiveMobile, 2011 [accessed 2011-10-01]. <http://www.adaptivemobile.com/global-security-insight-centre>.
19. Goldberg, I., Hill, A., Shostack, A. *Trust, Ethics and Privacy*. Boston University Law Review, 2001.
20. Hamblen, M. *McNealy calls for smart cards to help security* [interactive]. Computerworld, October 21, 2001 [accessed 2011-10-01]. <http://www.computerworld.com/s/article/64729/McNealy_calls_for_smart_cards_to_help_security>.
21. Liebowitz, M. *Google's Android Phones Track You Just Like iPhones* [interactive]. Security News Daily, Apr 22, 2011 [accessed 2011-10-01]. <http://www.securitynewsdaily.com/googles-android-phones-track-you-just-like-iphones-0720/>.
22. Nevin, Ch. *Taking liberties* [interactive]. The Economist: *Intelligent Life Magazine***,** Summer 2009 [accessed 2011-10-01]. <http://moreintelligentlife.com/content/charles-nevin/taking-liberties>.
23. Nissenbaum, H. *Privacy in Context California*. Stanford: Stanford University Press, 2010.
24. Penenberg, A. *Cookie Monsters* [interactive]. Slate, 7 Nov 2005 [accessed 2011-10-01]. <http://www.slate.com/articles/technology/technology/2005/11/cookie_monsters.html>.
25. Rambam, S. *Privacy is dead! Get over it!* [interactive]. Loss of Privacy, November 28, 2010 [accessed 2011-10-01]. <http://www.lossofprivacy.com/index.php/2010/11/steve-rambam-privacy-is-dead-get-over-it/>.
26. Ruebhausen, O.M. and Brim, O.G. *Privacy and Behavioral Research*. Columbia Law Review, 1965.
27. Specter, M. *Postcard from Silicon Valley*. The New Yorker, Spring 2000.
28. Walsh, J. *Paul Chambers: "privacy is dead, get over it" is not good enough* [interactive]. Globalcomment, January 19, 2010 [accessed 2011-10-01]. <http://globalcomment.com/2010/paul-chambers-privacy-is-dead-get-over-it-is-not-good-enough/>.
29. *Web attack knows where you live* [interactive]. BBC News Technology , August 3, 2010 [accessed 2010-10-01]. <http://www.bbc.co.uk/news/technology-10850875>.
30. Westin, A. *Privacy and Freedom*. New York: Atheneum, 1967.

TEISĖS Į PRIVATUMĄ RIBOJIMAS ELEKTRONINĖJE ERDVĖJE

Birutė Pranevičienė*
Mykolas Romeris University

Darius Amilevičius**
Mykolas Romeris University

S a n t r a u k a

Teisė į privatumą asmenims, socialinėms grupėms arba institucijoms suteikia teisę reikalauti, kad būtų nustatyta kada, kaip ir kokia apimtimi informacija apie juos gali būti atskleidžiama kitiems. Privataus gyvenimo laisvė - tai visuotinai naudingas pripažinimas, kad yra egzistencinė erdvė, kuri priklauso tik individui ir kiti neturi teisės į ją brautis. Šiais laikais internete žmogaus teisė į privatumą internete yra labai ribojama. Grėsmė interneto vartotojų privatumui nuolat didėja. Vystantis informacinėms technologijoms, galimybė rinkti duomenis, juos saugoti, suderinti tarpusavyje ir panaudoti šią informaciją tapo labai nesudėtinga operacija. Saityne egzistuoja milžiniškos duomenų bazės, kuriose saugoma milžiniški kiekiai įrašų su informacija apie internautų finansus ir kreditus, jų medicininiai įrašai, duomenys apie pirkimus ir telefoninius skambučius ir t.t. Dauguma žmonių net nežino, kokią informaciją apie juos turi ir saugo Interneto paslaugų teikėjai, nežino kas turi prieigą prie jų duomenų. Dabartinė teisinė bazė, reglamentuojanti elektroninę erdvę ir veiklą joje, nepakankamai veiksminga, todėl nėra teisinių priemonių, galinčių pažaboti interneto paslaugų teikėjų piktnaudžiavimą interneto vartotojų asmens duomenimis.

Teisė į privatumą nėra absoliuti teisė, kitaip tariant, visuomenė gali nustatyti jos apribojimus. Vyriausybė gali nuspręsti ir išleisti įstatymus, kurie riboja teisę į privatumą tam tikrais būdais ir tam tikrais atvejais. Kai asmuo ar valstybė įsiskverbia į kieno nors privačią erdvę, visada atsiranda vertybių hierarchijos dilema. Įvairios teisinės doktrinos lemia konkretaus įsiveržimo į asmens privatumą atvejo sprendimo pobūdį.

Nuolat didėjanti kriminalinių nusikaltimų ir terorizmo grėsmė verčia griežtinti įstatymų reikalavimus. Po 2001 metų rugsėjo 11 dienos teroristų išpuolių Niujorke, viso pasaulio visuomenė turėjo iš naujo apsvarstyti su informacijos saugojimu ir naudojimu susijusias taisykles ir metodus. Tai lėmė, kad vyriausybės pradėjo riboti žmogaus teisę į privatumą internete.

Taigi, viena vertus, egzistuoja Visuotinė žmogaus teisių deklaracija, Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, žmogaus teisių doktrinos ir t.t., kurios gina žmogaus teisę į privatumą klasikine šios sąvokos prasme. Iš kitos pusės, valstybės ir įstatymai, kurie turi ginti žmogaus teisę į privatumą, šią teisę pradėjo riboti.

Kriminalinių nusikaltimų ir teroristų grėsmės kontekste visuomenei nerimą kelia jos nacionalinis ir kiekvieno piliečio asmeninis saugumas. Jaunoji karta jau kitaip supranta „privatumą“ (šioje srityje moksliniai tyrimai vis dar nepakankami ir reikalauja didesnio mokslininkų dėmesio). Galime teigti, kad, tam tikra prasme, teisiniai teisės į privatumą ribojimai internete, vykdomi stiprinant nacionalinį saugumą, pasitarnauja interneto paslaugų teikėjams, kurie internautų teisę į privatumą riboja, siekdami komercinės naudos. Galime teigti, kad informacinei erai keičiant industrinę, būtina persvarstyti ir keisti sąvokos „privatumas“ prasmę, nes jau pastebimas savaiminis privatumo paradigmos pokyčio vyksmas.

Pagrindinės sąvokos: elektroninė erdvė, žmogaus teisės, privatumas, saugumas.

Birutė Pranevičienė*, Mykolo Romerio universiteto Viešojo saugumo fakulteto Teisės katedros profesorė. Mokslinių tyrimų kryptys: administracinė teisė, konstitucinė teisė.

Birutė Pranevičienė*, Mykolas Romeris University, Faculty of Public security, Department of Law, professor. Research interests: administrative law, constitutional law.

Darius Amilevičius**, Mykolo Romerio universiteto Viešojo saugumo fakulteto Humanitarinių mokslų katedros docentas. Mokslinių tyrimų kryptys: politinė ir juridinė retorika, semantinės ir kalbų technologijos, marketinginė komunikacija, žmogaus teisės.

Darius Amilevičius**, Mykolas Romeris University, Faculty of Public security, Department of Humanities, assoc. professor. Research interests: political and juridical rhetoric, semantic and natural language technologies, marketing communication, human rights.