Sosyo Ekonomi

Temmuz-Aralık 2012-2

Expectation of Privacy in Cyberspace: The Fourth Amendment of the US Constitution and an Evaluation of the Turkish Case

İlker PEKGÖZLÜ
ipekgozlu@egm.gov.tr

Mustafa Kemal ÖKTEM
kemalok@hacettepe.edu.tr

Sanal Ortamda Mahremiyet Beklentisi: Amerikan Anayasası'nın Ek Dördüncü Maddesi ve Türkiye'deki Durumun Değerlendirilmesi

Abstract

Privacy in cyberspace is becoming a dispute issue for the criminal justice system. Initially, we should determine what kind of cyberspace we desire, and then, we can choose a legal platform to get this online environment. Because policing in cyberspace is an inevitable need, the question of what extent the law can protect individuals' expectation of privacy in cyberspace has become an important problem. This study initially explains the legal descriptions of privacy, expectation of privacy, and cyberspace. Then, it discusses the expectation of privacy in cyberspace based on the Fourth Amendment of the United States Constitution. It also presents the current state of the privacy of private life and the privacy of communication in the Turkish judicial system.

Keywords : e-Privacy, e-Government, Turkish Public Administration.

JEL Classification Codes : M15, K11, K23, K42.

Özet

Sanal âlemde kişisel giz alanı, ceza adalet sistemi açısından tartışmalı bir konu haline gelmektedir. Öncelikle, ne tür bir sanal âlem arzu ettiğimize karar vermeliyiz ve daha sonra bunu çevrimiçi ortama aktarmak için yasal bir dayanak seçebiliriz. Sanal âlemde güvenliği sağlamak kaçınılmaz bir gereksinim olduğu için hukukun sanal âlemde bireylerin giz beklentisini hangi ölçüde koruyabileceği önemli bir sorun olmuştur. Bu çalışma başlangıçta kişisel giz, giz beklentisi ve sanal âlemin hukuksal tanımlarını açıklamaktadır. Daha sonra Amerika Birleşik Devletleri Anayasası'nın dördüncü ilave maddesi çerçevesinde sanal âlemde giz beklentisini tartışmaktadır. Çalışma aynı zamanda Türk adalet sisteminde bugünkü özel yaşamın gizliliği ve iletişim gizliliğini ortaya koymaktadır.

Anahtar Sözcükler : e-Mahremiyet, e-Devlet, Türk Kamu Yönetimi.

Acknowledgement

Initial version of this paper has been presented to the "*MIC 2010 Management International Conference on Social Responsibility, Professional Ethics, and Management*" organized by University of Primoska, University Emuni and Hacettepe University in Ankara on 24-27 November 2010.

Beyan

Bu makalenin ilk hali, Primoska Üniversitesi, Emuni Üniversitesi ve Hacettepe Üniversitesi tarafından Ankara'da 24–27 Kasım 2010'da düzenlenen "*MIC 2010 Kurumsal Sosyal Sorumluluk, Mesleki Etik ve Yönetim konulu Uluslararası Yönetim Konferansı*"na sunulmuştur.

1. Introduction

While civilization progresses, generally, old but not aging concepts meet to new ones. A fundamental human right "privacy" is becoming a dispute issue for professional ethics, the criminal justice system, management of public organizations, and information society since electronic communication has brought a new notion called "cyberspace."

As communications and markets are moving into this electronic realm, and millions of people in the world communicate using the Internet, cyberspace is turning into a place in which many crimes can be committed easily. Therefore, it is inevitable for law enforcement officials to monitor and engage investigations in the Internet. However, these investigations can cause intrusions to privacy domains of individuals.

Regarding expectation of privacy in cyberspace issue, Grosso (1994) comments "[w]henever new technology becomes prevalent, the law enters a period of struggle to find adequate means for resolving disputes involving that technology, and for protecting the rights of people affected by it. We are now in such a period."

Initially, we should determine what kind of cyberspace we desire, and then, we can choose a legal platform to get this online environment. Because policing in cyberspace is an inevitable need, the question of what extent the law can protect individuals' expectation of privacy in cyberspace becomes an important issue.

2. The Concepts of Privacy, Expectation of Privacy, and Cyberspace

Legal descriptions are required in order to understand concepts in connection with privacy, expectation of privacy, and cyberspace. In Black's Law Dictionary, privacy is described as;

> "the condition or state of being free from public attention to intrusion into or interference with one's acts or decisions" (Garner, 2004).

In the realm of privacy in cyberspace, the important issue is the protection of informational privacy. In Black's Law Dictionary, informational privacy is described as;

> "a private person's right to choose to determine whether, how, and, to what extent information about oneself is communicated to others, especially sensitive and confidential information" (Garner, 2004).

Katyal (2003) writes that at first, informational privacy developed under the conception that personal papers completely and clearly identified the people whose lives they explained. However, "today, the perception of informational privacy extends, at least in cyberspace, to something quite different: It covers the very act of creating fictive personalities, in addition to the possibility of anonymously publishing information online" (Katyal, 2003).

When the issue is about expectation of privacy in cyberspace, the concept of expectation of privacy should be considered as well. In Black's Law Dictionary, expectation of privacy is described as;

> "a belief in the existence of the right to be free of governmental intrusion in regard to a particular place or thing" (Garner, 2004).

Reasonable expectation of privacy is affected by information and communication technologies which influence human capabilities to access information at a distance. As a result, space is no longer a marker for showing boundaries between private and public interactions. In the new world of information and communication, the private objects, such as electronic files, are quite different from objects, such as physical and tangible objects, which were formerly the subjects of privacy (Waldo, Lin, and Millett, 2010).

On the other hand, the Internet and cyberspace are necessary concepts in the issue of expectation of privacy in cyberspace. According to the court in *American Civil Liberties Union v. Reno* "the Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks" (American Civil Liberties Union v. Reno, 1996).

Although some technical distinctions exist between them, the terms of "cyberspace" and "Internet" are used interchangeably as referring to the virtual space created by "the (potential) interconnection between any of millions of computers located around the world" (Froomkin, 2003).

Yen (2002) describes cyberspace as "the virtual space created by operation of the Internet, a network of computers that share information with each other."

Ferrera et al. (2001) explain that cyberspace is the "term originally used by William Gibson in his 1982 novel *Neuromanner*. The totality of all the world's computers, represented as a visual virtual three dimensional domain in which a user may move and act with the consequences in the real world."

According to Gleason and Friedman (2004), the challenge in conception of cyberspace is to define it positively. The first step to express clearly an accessible conception of cyberspace is to define what cyberspace is not.

> "It is not the physical world, and it is not a 'parallel universe.' It is not the creation of any one person or group of persons. It is not its protocols, and it is not the machines or software on which it runs. It is connected to all these things, and yet it is something transcendent; it is neither purely technical space nor purely social" (Gleason and Friedman, 2004).

There are different methods of communication and information exchange over the network for the Internet users. Since the methods of communication and information access are continually developing, it is not easy to categorize in brief. The most common methods of communications on the Internet can be generally grouped into six categories:

> (1) one-to-one messaging (such as "e-mail"), (2) one-to-many messaging (such as "listserv"), (3) distributed message databases (such as "USENET newsgroups"), (4) real time communication (such as "Internet Relay Chat"), (5) real time remote computer utilization (such as "telnet"), and (6) remote information retrieval (such as "ftp," "gopher," and the "World Wide Web"). In order to transmit data, text, visual images, computer programs, sound, and moving video images, these methods of communication can be used (American Civil Liberties Union v. Reno, 1996).

There are efforts to secure privacy in cyberspace. According to Harvard Law Review Association (1997), mainly, three methods are used to restrict access to the Internet communication. The basic way is "security through obscurity." This approach assumes that communication will be protected if it is not known by the public where the message is. However, the secrecy cannot be guaranteed since someone can leak the location. Therefore, this approach is not effective for privacy (Harvard Law Review Association, 1997). The second way is using a gateway that requires the Internet user to submit certain information before going on any further. Some gateways only ask user to confirm some information, which is ineffective method. However, some gateways use complex techniques that requires password for access (Lessig, 1996).

There is still privacy problem since "hackers" may try to get password to break into the system (Harvard Law Review Association, 1997). Encryption is another method of restricting access to cyberspace communication. There are many kinds of encryption ranging from the use of foreign languages to simple mathematical codes to complex algorithms. Without a key, it is very difficult to decode these encryptions (Grosso, 1994). Since the system administrator is able to monitor all information transmitted into or out of

the network, each of these methods of securing privacy in cyberspace is limited (Harvard Law Review Association, 1997).

3. Legal Basis

The Fourth Amendment to the United States Constitution constitutes "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." With considering the explanation of expectation of privacy above, the Fourth Amendment protects people against unreasonable searches and seizures of government officials. In connection with the privacy, the concept of house is very important in the Fourth Amendment. Because the intention was to protect against property-based warrants, early Fourth Amendment jurisprudence concentrated on requirements of space and place (Hunter, 2003). Specifically, the three basic spaces of protection are the individuals' physical selves ("persons"), their real property ("houses"), and their personal property ("papers, and effects") (Hunter, 2003).

However, according to Seidman, the Fourth Amendment does not protect informational privacy per se (Seidman, 1995). Modern Fourth Amendment law assumes that because the government is entitled to seize any item that is useful in any way to a criminal investigation, the government can access to information if a need can be established (Seidman, 1995).

Initially, the Supreme Court assessed the Fourth Amendment in the perspective of a location. In *Olmstead v. United States*, the Court showed this assessment when it allowed government officials to wiretap the suspects' houses (Olmstead v. United States, 1928). The Supreme Court found no Fourth Amendment violation when wiretapping since there was no trespass into a constitutionally protected area (Olmstead v. United States, 1928). Even though, firstly, in *Olmstead v. United States* only inspections that physically trespassed upon constitutionally protected areas were considered "searches," in *Katz v. United States*, the Supreme Court set up that an inspection may be a search regardless of any physical invasion (Katz v. United States, 1967).

In *Katz v. United States*, the Supreme Court held that no physical trespass is required to violate the Fourth Amendment. The Constitution protects people, not places; thus, the Fourth Amendment protection is with person wherever he or she goes (Katz v. United States, 1967). The Court maintained that as long as their behaviors give them expectation of privacy, people are entitled to a reasonable expectation of privacy wherever they may be (Katz v. United States, 1967).

In *Katz v. United States*, the Court set up a two-part test to determine whether a protected privacy interest exists: (1) whether a person has displayed an "actual (subjective) expectation of privacy" and (2) whether that "expectation be one that society is prepared to recognize as reasonable" (Katz v. United States, 1967).

The existence of a legitimate expectation of privacy is subject to a main restriction: "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected" (Katz v. United States, 1967).

The case of *Kyllo v. United States* addresses the use of the thermal imaging devices in law enforcement to detect heat signatures radiating from a house for the purposes of drug prevention (Kyllo v. United States, 2001). The issue was whether the use of a device that was not in general public use to explore details of a private home constitutes an unreasonable search. The Court held that the use of thermal imaging technology to detect heat signatures radiating from a house was a search although the device could not penetrate the walls of the house (Kyllo v. United States, 2001).

According to Harvard Law Review Association (1997), when resolving the scope of the Fourth Amendment, courts and writers have generally put similarities from previous court examples. For instance, commentators have compared e-mail to postal mail. Persons have a reasonable expectation of privacy in sealed first-class mail sent through the postal system. However, since anyone can read the contents of a postcard, an expectation of privacy in its contents would be unreasonable and a law enforcement officer's reading it is, therefore, not a search (Harvard Law Review Association, 1997).

One approach is that e-mail, which "can be accessed or viewed on intermediate computers between the sender and recipient unless message is encrypted," may more closely look like a postcard than a letter (American Civil Liberties Union v. Reno, 1996). However, an e-mail can take many different paths between its source and destination computers (American Civil Liberties Union v. Reno, 1996). Each message is divided into small packets that are transmitted separately probably along different route. Therefore, only the sender and recipient can receive the actual message. An expectation of privacy in the e-mail message may be reasonable if system administrators on these computers have accepted not to read e-mails (Harvard Law Review Association, 1997). On the other hand, when the recipient opens the e-mail, the government officials may get the e-mail from the recipient or seize the recipient's copy of the e-mail. In this regard, there is no the Fourth Amendment violation. e-Mails sent to large numbers of persons also do not have the Fourth Amendment protection (United States v. Maxwell, 1996).

The second analogy makes comparison between cyberspace communication and telephone calls (American Civil Liberties Union v. Reno, 1996). After *Katz v. United States,* the Supreme Court has ruled that a person's expectation of privacy in land-wired telephone calls is reasonable (Katz v. United States, 1967). However, lower courts have recognized as unreasonable an individual's expectation of privacy in cordless telephone calls (McKamey v. Roach, 1995; Tyler v. Berodt, 1989). According to the U.S. Court of Appeals (Fifth Circuit) whether an expectation of privacy in a conversation on a cordless phone is reasonable will depend upon the particular characteristics of the phone (United States v. Smith, 1992). Even though cyberspace communication may be captured along the road of transmission, whether the possibility of such interception is big enough to turn into an expectation of privacy unreasonable is unclear (Harvard Law Review Association, 1997).

The third analogy holds cyberspace as a place. Even though in *Katz v. United States,* the Supreme Court held that "the Fourth Amendment protects people, not places," the Amendment protects privacy to some degree, which is related to the place inspected (Katz v. United States, 1967). Courts and commentators declare that the protection of the home privacy (Payton v. New York, 1980) does not constitute a reasonable expectation of privacy in "open fields" although a fence and "no trespassing" signs exist (Oliver v. United States, 1984). However, since the structure of cyberspace is different from traditional places, it has important restrictions to compare cyberspace to a place that the Fourth Amendment protects. Finally, these similarities do not give a clear structure to apply the Fourth Amendment rules in cyberspace (Harvard Law Review Association, 1997).

Another debating issue is encryption in cyberspace. Kerr explains that even though the Internet is a recent concept that has brought about revolutionary change, some debates regarding the Fourth Amendment caused by encrypting Internet communications are not new. The cases in which the Fourth Amendment was applied disclosure that decrypting an Internet communication cannot itself transgress a "reasonable expectation of privacy" and thus cannot violate the Fourth Amendment. Consequently, decrypting Internet communications by government officials do not constitute a violation of the Constitution (Kerr, 2001).

Regarding expectation of privacy in cyberspace, the other issue is chat rooms. In *U.S. v. Charbonneau*, the District Court ruled that "when [a person] engages in [a] chat room conversations, [he or she] runs the risk of speaking to an undercover agent. Furthermore, [this person] cannot have a reasonable expectation of privacy in the chat rooms. In addition, all e-mail sent or forwarded to the undercover agents is not protected by the Fourth Amendment" (U.S. v. Charbonneau, 1997).

Similarly, many cases show that communicating with large groups in the Internet is not protected by the Fourth Amendment (Kerr, 2010). Kerr (2010) argues that an Internet user has no Fourth Amendment rights if he or she posts information on a public web page (United States v. Gines-Perez, 2002). Kerr (2010) also discusses that reasonable expectation of privacy is waived when an individual shares files with others on an open computer network (United States v. King, 2007). Kerr (2010) additionally explains that if an individual sends a message to a large group which includes a confidential informant, the message can be read and sent to the police by the informant without violating the Fourth Amendment (Hoffa v. United States, 1966; United States v. King, 1995).

There are exceptions to the Fourth Amendment's warrant requirement and three of them are important in cyberspace issue: (1) when consent to search has been given (Schneckloth v. Bustamonte, 1973), (2) when the information has been disclosed to a third party (United States v. Miller, 1976), and (3) when the information is in plain view of an officer (Horton v. California, 1990). There is no warrant requirement when a sender gives consent to a law enforcement officer to read the communication (Schneckloth v. Bustamonte, 1973).

Although the sender does not give any consent to a search, a third party who has the authority of search over the object may search. A third party's authority to consent is based "on mutual use of the property by persons generally having joint access or control for most purposes" (United States v. Matlock, 1974). On a computer network, "[w]hether the system manager has the right to consent will depend upon how the rights of access and control are allocated between the system manager and the user" (Sergent, 1995).

The last exception is the plain view exception, which may apply "objects, activities, or statements that [a person] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited" (Katz v. United States, 1967). The simple observation of an object in plain view is not a search (Horton v. California, 1990). Since public can access to the Internet freely, law enforcement agents have no less right to browse the Internet than other persons do. In addition, expectation of informational privacy in a place that public can observe plainly by browsing is unreasonable, and "once someone places data or other evidence onto a computer in a publicly-accessible manner, they lose any expectation of privacy in the information" (Winick, 1994).

4. Concluding Remarks and Implications for the Turkish Case

Even if the Internet communication holds necessary conditions of privacy such as password protection, courts could claim many reasons to rule that no reasonable expectation of privacy exist in cyberspace communication. One reason is that users are

aware of interception by various unspecified system administrators in any Internet communication; therefore, in this condition, there is no reasonable expectation of privacy. The other reason is that there are backup files, which are automatically stored on the network, and users have no standing to object to the search of these backup files. Another important reason is that computer network is a new concept for society in connection with expectation of privacy in the communication (Harvard Law Review Association, 1997).

Kerr discusses whether the Fourth Amendment is a sufficient means for protecting privacy in cyberspace, and writes that since the judges do not want to establish one Fourth Amendment for the physical world and another for cyberspace, they will enforce the physical world's standards constituted by the Fourth Amendment to the Internet world (Kerr, 2001). Continuing, Kerr suggests that this approach may give some confusing outcomes, and writes "[w]hat we expect would be protected by the Fourth Amendment may not be" (Kerr, 2001). In addition to Kerr's discussion, Katyal (2003) comments although many persons insist on keeping a reasonable expectation of anonymity and share files in cyberspace, it is unclear whether an individual can hold both rights simultaneously.

As Kerr (2010) suggests based on LaFave et al.'s comments that currently, it is highly unclear how the Fourth Amendment applies to the government surveillance of Internet communications. He discusses two explanations for the reasons. First, when Congress enacted the Electronic Communications Privacy Act in 1986, it extended the electronic surveillance statutes to e-mail messages and computer. Since the statute clearly protects the rights, possible constitutional challenges of its less protection compared to the Fourth Amendment have not drawn attention. Second, child pornography offense, the most common type of computer crime, is mostly related to search and seizure of stand-alone computers instead of online surveillance. Therefore, "the Fourth Amendment rules governing online surveillance have remained largely unexplored" (Kerr, 2010).

It is clear that privacy in cyberspace is continuing to become more important and frail issue. Depending on developing technology and new different situations, the interpretations of the Constitution can be difficult to hold cases.

While cyberspace is becoming a real fact into all persons' lives, not only the criminal justice system of the United States but also the judicial system in Turkey should adapt itself to this change by balancing the rights and the rules.

In the Turkish case, there are at least two different approaches for any legal problem in social life: One is to regulate any problem by passing a new law (however, on e-communication matters there is a lack of even new legal regulations, since the judicial system could naturally not keep up with new technological developments); and on the

contrary, the second opinion is that it is not possible to prevent any misconduct on information privacy by new laws.

This second idea would be based on a view that Turkish society and administrative system is different than any European country or the U.S. Thus, making new laws would not be enough; for example, it is critical to inhibit any illegal interception to privacy through some technological devices, which are legally or illegally available in the market (or sometimes in the black-market). This opinion defends that it is important to have a strong political desire to take care of privacy matters in the society.

If we remember Gleason and Friedman's (2004) conception of cyberspace again and try to formulate it in a more tangible perspective, it is almost non-existent, it is in nowhere, but in fact it is everywhere, and it is strongly influential in citizens' lives: "It is both the physical world and a 'parallel universe.' It is connected to all such elements: the creation of one person or group of persons, protocols, the machines and software on which it runs, and yet it is something transcendent. However, it is neither purely technical space nor purely social." For that reason, it is even more difficult to define, diagnose, limit, compensate, decide, and manage it. It takes more courage and professionalism to handle it properly in a manner to best suit to the people's needs and balance public interest.

In this regards, Turkish Constitution of 1982 has faced a hot debate recently, and some articles on basic rights and their amendments were voted in September 2010 referendum in the search of better protecting basic rights and a more democratic system. Amendment 2 for article 20 brought an additional paragraph on privacy rights[1], and states that this issue shall be regulated by law in detail. Even so, no amendment is complete. There will be always a need for better frameworks.

The protection of individual privacy against intrusions and assaults has been also discussed by academicians and practitioners in Turkey. Although there are different types of intrusions to privacy domains of persons, these intrusions can be categorized under three topics: secretly accessing to privacy domain of individual, recording by technical devices, and dissemination and transmission (Zevkliler, Acabey, and Gökyayla, 1999: 468-475).

---

[1] *Amendment 2: Everyone has the right to demand the protection of his or her personal information. This right also involves to be informed about the information related to one's own, access to this information, to request their correction and deletion and to know about whether these data are utilized in accordance with the purposes. Personal information shall only be processed in accordance with the conditions anticipated by law or with the express consent of the person. Principles and procedures on the protection of personal information shall be regulated by law.*

The privacy area of a person can be secretly accessed by secretly listening, observing, or reading individual letters, memories, or documents. Even though a person can be listened simply by ear, some technical devices can be used for secret listening. While entering one's house or office without consent of that person and reading his or her personal letters or papers is considered as intrusion to privacy, reading these papers by seizing his or her communication tools or devices is also deemed as intrusion to personal privacy (Zevkliler, Acabey, and Gökyayla, 1999: 468).

Actions related to recording private papers, pictures, videos, or talks secretly include not only secretly accessing to privacy domain of a person but also recording these private and personal data and information on tapes, films, or similar backup devices. In that case, these records are always kept by the perpetrator which means there is an ongoing assault (Zevkliler, Acabey, and Gökyayla, 1999: 469).

Distributing a person's letters, memories, papers, videos, pictures, or sound records to other people or broadcasting these personal private items to the community is also a kind of intrusion to privacy domain of individual, which is discussed under the topic of dissemination and transmission. When a person gives consent to be published his or her documents, memories, speech, or images, publishing these personal items in a way which is different from the way permitted by the person is also considered as a type of intrusion to privacy (Zevkliler, Acabey, and Gökyayla, 1999: 469).

Actually, the privacy issue was assured by different laws in Turkey. Persons are protected against intrusions to privacy domains of individuals primarily by the Constitution (Article 15–17) and Civil Code (Article 24), and by other laws such as, Penal Code, Intellectual Property Act, and Code of Obligations (Zevkliler, Acabey, and Gökyayla, 1999). For example, according to the Article 15 of the Constitution (TC Anayasa Mahkemesi, 2011), "... the individual's right to life, and the integrity of his or her material and spiritual entity shall be inviolable...," and the Article 17 of the Constitution (TC Anayasa Mahkemesi, 2011) constitutes "[e]veryone has the right to life and the right to protect and develop his material and spiritual entity." Similarly, according to the Article 24 of Civil Code (TÜSEV, 2011), "[t]he person subject to assault on his/her personal rights may claim protection from the judge against the individuals who made the assault. Each assault against personal rights is considered contrary to the laws unless the assent of the person whose personal right is damaged is based on any one of the reasons related to private or public interest and use of authorization conferred upon by the laws."

Additionally, “Information Access Right Law No. 4982 of 2003” and the by-law (Regulation for Implementing the Information Access Right Law, 2004) on its implementation has endeavored to give citizens the right to demand information on acts and actions of public administration, which has enormous resources and records of

information including private data. The article 22[2] has excluded access to communication privacy. The article 21[3] deals with privacy of private life, and it draws the private sphere as information records on personal health, private and family life, and personal honor, professional and financial documents to protect unjust competition.

Turkish Information and Communication Technologies Authority[4] makes a definition on privacy by its ordinance[5] such as; "Personal Information/Data: Any information related with real and/or legal persons which can be defined directly or indirectly by using one or more elements of identity card number or physical, psychological, intellectual, economic, cultural and social identities or health related, genetic, ethnic, religious, family related and political information."

Although we would also love to power the country's future with technology as in the U.S. (Swire, 2009)[6], where e-Government Act of 2002 has went into effect (Swire, 2009)[7], unfortunately, in Turkey, a law on e-government with a precise definition of its processes and procedures has not been yet enacted. Moreover, we should be deeming of another step forward and try to take measures on how to require use of "privacy impact assessments" (Swire, 2009)[8] for new computer systems as to become a best practice for public administration.

Academicians and practitioners should work together for public service by re-conceptualizing how to formulate new regulations on privacy and how to apply them in today's high-technology background. The emerging problems are believed to be overcome

---

2 *The privacy of communication: Article 22: Information and documents that would violate the basis of communication privacy are beyond the scope of the information access right.*

3 *The privacy of private life: Article 21: With the proviso where the consent of the concerned individual has been received, the information and documents that will unjustly interfere with the health records, private and family life, honour and dignity, and the economical and professional interests of an individual, are out of the scope of the right to information. Due to public interest considerations, personal information or documents may be disclosed by the institutions on the condition that concerned individual is notified of the disclosure at least 7 days in advance and his/her written consent is obtained.*

4 *There is a criticism that the establishing law for this Authority has been amended and rejected, but the legislation has not yet been finalized to clearly define and limit boundaries of privacy.*

5 *According to the Unofficial Translation of Ordinance on Personal Information Processing and Protection of Privacy in The Telecommunications Sector (prepared on the basis of Telegram and Telephone Law No: 406 of 4/2/1924 and Wireless Law No: 2813 of 15/4/1983); this ordinance covers real and legal persons providing or using services in the telecommunications sector, accessed on 27.8.2010: (http://www.tk.gov.tr/eng/pdf/data_protection.pdf).*

6 *Please see: http://www.whitehouse.gov/omb/egov/index.html in Swire (2009).*

7 *Pub. L. No. 107-347, 116 Stat. 2899, 2002 in Swire (2009).*

8 *R. Steve Edmondson, Ohio Off. Info. Tech., Privacy Impact Assessments (2008), (http:// www.oit.ohio.gov/IGD/policy/pdfs_bulletins/ITB-2008.02.pdf (implementing statutory requirements) in Swire (2009).*

by introducing some new principles like the "Proportionality Principle" (Swire, 2009), which "applies to government access to personal data" "where greater intrusiveness of government action leads to greater safeguards", "to review the propriety of sanctions" and "to measure the legality of a wide range of government conduct through some form of means-ends analyses", as a general principle of public law, applicable to constitutional law, also to administrative law for government surveillance systems, "with a rational bureaucratic process to ensure that the intrusiveness of the systems is matched with proportionate procedural protections".

The next challenge would be to integrate Turkish privacy protection system into the broader international debate, for example with European countries. Swire (2009) reminds that "the Europeans create legal protections, and those structures appear stable and workable[9]."

References

American Civil Liberties Union v. Reno, 929 F.Supp. 824, E.D.Pa. (1996).

Ferrera G.R., S.D. Lichtenstein, M.E.K. Reder, R. August, and W.T. Schiano (2001), *CyberLaw: Your Rights in Cyberspace*, Mason, OH: Thomson Learning.

Froomkin, A.M. (2003), "Habermas @Discourse.net: Toward a Critical Theory of Cyberspace", *116 Harv. L. Rev.*, 749-78.

Garner, B.A. (2004), *Black's Law Dictionary,* 8th edition. USA: Thomson-West.

Gleason, D.H. and L. Friedman (2004), "Toward an Accessible Conception of Cyberspace", *28 Vt. L. Rev.*, 299-320.

Grosso, A. (1994), "The National Information Infrastructure", 41 Fed. B. News & J., 481, 485-86.

Harvard Law Review Association (1997), "Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication", *110 Harv. L. Rev.,* 1591- 1608.

Hoffa v. United States, 385 U.S. 293, 300–03 (1966).

Horton v. California, 496 U.S. 128, 133 & n.5. (1990).

---

[9] *European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Apr. 11, 1950, C.E.T.S. 005: 1) everyone has the right to respect for his private and family life, his home and his correspondence. 2) 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 freedoms of others.*

Hunter, D. (2003), "Cyberspace as Place and the Tragedy of the Digital Anticommons", *91 Cal. L. Rev.,* 439-519.

Katyal, S.K. (2003), "The New Surveillance", *54 Case W. Res. L. Rev.,* 297.

Katz v. United States, 389 U.S. 347 (1967).

Kerr, O.S. (2001), "The Fourth Amendment in Cyberspace: Can Encryption Create a 'Reasonable Expectation of Privacy?'", *33 Conn. L. Rev.,* 503-533.

Kerr, O.S. (2010), "Applying the Fourth Amendment to the Internet: A General Approach", *62 Stan. L. Rev.,* 1005.

Kyllo v. United States, 533 U.S. 27 (2001).

Lessig, L. (1996), "Reading the Constitution in Cyberspace", *45 Emory L.J.,* 869-91.

McKamey v. Roach, 55 F.3d 1236, 1239 (6th Cir. 1995).

Oliver v. United States, 466 U.S. 170, 179 (1984).

Olmstead v. United States, 277 U.S. 438, 466 (1928).

Payton v. New York, 445 U.S. 573, 589 (1980).

Regulation for Implementing the Information Access Right Law (2004), Order Number: 2004/7189, 19.4.2004.

Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

Seidman, L.M. (1995), "The Problems with Privacy's Problem", *93 Mich. L. Rev.,* 1079-1086.

Sergent, R.S. (1995), "A Fourth Amendment Model for Computer Networks and Data Privacy", *81 Va. L. Rev.,* 1181-1226.

Swire, P.P. (2009), "Review of Christopher Slobogin's Book (Privacy at Risk: The New Government Surveillance and the Fourth Amendment, University of Chicago Press 2007): Proportionality for High-Tech Searches", *Ohio State Journal of Criminal Law* 6, 751–63.

T.C. Anayasa Mahkemesi (2011), *The Constitution of the Republic of Turkey*, <http://www.anayasa.gov.tr/images/loaded/pdf_dosyalari/THE_CONSTITUTION_OF_THE_REPUBLIC_OF_TURKEY.pdf>, 28.02. 2011.

TÜSEV (2011), *Turkish Civil Code*, <http://www.tusev.org.tr/userfiles/image/turkey%20tr%20civil%20code%20provisions.pdf>, 28.02. 2011.

Tyler v. Berodt, 877 F.2d 705, 706–07 (8th Cir. 1989).

United States v. Gines-Perez, 214 F. Supp. 2d 205 (D.P.R. 2002).

United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995).

United States v. King, 509 F.3d 1338 (11th Cir. 2007).

United States v. Matlock, 415 U.S. 164, 171 (1974).

United States v. Maxwell, No. 95–0751, 1996 (C.A.A.F. Nov. 21, 1996).

United States v. Miller, 425 U.S. 435, 442–43 (1976).

United States v. Smith, 978 F.2d 171, 180 (5th Cir. 1992).

U.S. v. Charbonneau, 979 F.Supp. 1177 S.D.Ohio (1997).

Waldo, J., H.S. Lin, and L.I. Millett (2010), "Thinking About Privacy: Chapter 1 of 'Engaging Privacy and Information Technology in a Digital Age'", *Journal of Privacy and Confidentiality,* 2(1): 19–50.

Winick, R. (1994), "Searches and Seizures of Computers and Computer Data", *8 Harv. J.L. & Tech.,* 75, 81-82.

Yen, A.C. (2002), "Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace", *17 Berkeley Tech. L.J.,* 1207-1214.

Zevkliler, A., M.B. Acabey, K.E. Gökyayla (1999), *Zevkliler Medeni Hukuk,* Ankara: Seçkin Yayınevi.