

## *Chapter 20*

---

# **Communications Data Retention: A Pandora's Box for Rights and Liberties?**

---

*Lilian Mitrou*

### **Contents**

20.1	A New Age for Surveillance and Liberties? .....	410
20.2	Data Retention as a (Valuable?) Surveillance Tool .....	411
20.2.1	Communications and Traffic Data .....	412
20.2.2	Interception, Preservation, and Retention .....	413
20.3	European Regulatory Framework .....	414
20.3.1	Cybercrime Convention of the Council of Europe .....	414
20.3.2	Privacy and Electronic Communications Law in the European Union .....	415
20.3.2.1	The E-Privacy Directive: Data Retention as an Option .....	415
20.3.2.2	Mandatory, Routine Data Retention: The New Directive .....	416
20.3.3	Data Retention as Interference with the Right to the Respect of (Communicational) Privacy .....	418
20.4	Privacy and Electronic Communications Law in the United States .....	419

**410 ■ Digital Privacy: Theory, Technologies, and Practices**

20.4.1	The Legal Framework: The Electronic Communications Privacy Act .....	419
20.4.2	The Fourth Amendment and the “(Un)reasonable” Expectation of Communicational Privacy .....	420
20.5	New Challenges, Old Instruments: The Shortcoming of “Content-Envelope” Distinction .....	422
20.5.1	The Blurring Lines of “Content” and “Envelope” .....	422
20.5.2	A False Distinction? .....	423
20.6	Data Retention versus Fundamental Freedoms .....	424
20.6.1	An Unnecessary and Disproportionate Measure? .....	424
20.6.1.1	Criteria of “Acceptable” Interference .....	424
20.6.1.2	A Disproportionate “Dataveillance” .....	425
20.6.2	Communications Surveillance as Interference into the Rights of Anonymity and Freedom of Expression ...	426
20.6.3	The Question of Independent and Adequate Oversight .....	427
20.6.4	Common Information Pools for Public and Private Sector .....	428
20.7	An Information-Based (Pre)prevention of Risks or a Threat to Democracy .....	429
	References .....	430

**20.1 A New Age for Surveillance and Liberties?**

The internationally increased attention on organized crime, cyber-crime, as well as terrorism—reinforced by the terrorist attacks, especially in New York, Madrid, and London—have created a fertile ground for governments and international organizations to speed up the adoption of legislation that will strengthen the investigation and prosecution powers of enforcement authorities. The shock of terrorist attacks puts the subject of “security” thoroughly back on the political agenda and the public debate. In the wake of each attack, earlier proposals, which had “no chance to be accepted” [25,27], were reintroduced, and new policies with similar objectives were drafted to extend state surveillance authority. In the past five years, the legal and political landscapes have shifted significantly in many countries and at the international level, in order to face the new risks and threats and, in general, the problems that arise from the changing nature and type of criminal activity and terrorism.

The legal apparatus reflects new powers, investigative methods, and procedures that are supported, when not created, by a new technological environment. Technology has always been used to safeguard collective and individual security. However, new sophisticated technologies have

led to a profound increase in law enforcement surveillance, as they have given governments an unprecedented ability to engage in powerful mass surveillance [43]. The events of September 11 have facilitated and accelerated the move toward an intelligence-gathering form of policing [27]. The so-called “soft security measures” mainly seek to exploit the interactivity of information communication technologies in order to identify the risk-posing individuals and their networks [31].

The freedom of the individual and the security of all, i.e., the state’s tasks of guaranteeing individual, constitutionally protected freedoms, and of attending to and providing for the community’s security, are inevitably in a relationship marked by tension and even contradiction [17]. Surveillance measures raise significant concerns in relation to the respect of privacy and other fundamental rights and freedoms. This contribution deals with the question of data retention as a method of mass communications surveillance. In this chapter, I discuss the retention of communications data as a security measure, which interferes with the right to privacy. Privacy is perceived not as merely a right possessed by individuals, but as a prerequisite for making autonomous decisions, freely communicating with other persons, and being included in a participation society.

In Section 20.2, I examine communications monitoring as a law enforcement tool, by presenting the notions of interception of content, data retention, and data preservation. I consider critically the choices of legislators in the European Union and the United States (Sections 20.3 and 20.4), by referring to the legal framework and assessing the respective jurisprudence. Emphasis is given on the recently (2006) adopted EU Data Retention Directive and its effects on freedom of communication and privacy. In Section 20.5, assessed is the distinction of content and communications data, which forms the groundwork for the legislative options and judicial approaches. Further, I examine in Section 20.6 whether, and to what extent, the new legal landscape takes into account the values and fundamental rights deeply embedded in democratic societies and legal orders. Section 20.7 concludes the chapter by considering the far-reaching effects of mass surveillance on the relationship and the adjustment of freedom and security and consequently on the nature of state and society.

## **20.2 Data Retention as a (Valuable?) Surveillance Tool**

Access to communications data and its content has always been one of the most commonly used ways of gathering information for criminal investigations and the activities of intelligence services. In the emerging information society, more and more social interaction as well as business

relationships are conducted via electronic communications networks. As a result, traditional procedural measures of information collection through law enforcement authorities, such as search and seizure, have to be adapted to the dynamic nature of data and information flows and more generally to the new technological and societal environment [13].

If communications content is intercepted only in exceptional and specific cases, providers store the communications or transactional data routinely for the purposes of conveying and billing of communications. In the context of prevention, investigation, detection, and prosecution of criminal offenses and/or terrorist attacks (committed or supported by means of electronic communication networks), data relating to the use of communications are valuable in tracing and locating the source and the route of information as well as collecting and securing evidence. The retention of this data is pivotal to reactive investigations into serious crimes and the development of proactive intelligence on matters affecting not only organized criminal activity, but also national security [8].

### **20.2.1 Communications and Traffic Data**

A lot of confusion exists about the notion of this data, as the definitions in various national and/or international legal texts are quite different [12]. The provisions of the EU e-Privacy Directive relate to “traffic data” as “any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof” (Art. 2 b). The e-Privacy Directive covers all traffic data “in a technology neutral way,” i.e., those of traditional circuit-switched telephony as well as packet-switched Internet transmission. Different communications infrastructures give rise to different forms of transactional data [37]. “Traffic data, among other things, may consist of data referring to the routing, duration, time, or volume of a communication; to the protocol used; to the location of the terminal equipment of the sender or recipient (location data); to the network on which the communication originates or terminates; to the beginning, end, or duration of a connection. It may also consist of the format in which the communication is conveyed by the network” (2002/58/EC Recital 15). However, the European Data Retention Directive refers not only to “traffic data,” but also to any related data necessary to identify the subscriber or user (data necessary to identify the source and the destination of a communication, such as the name and address of the subscriber or registered user). To the extent that this data is relating to an identified or identifiable natural person, it is deemed to be “personal data,” as defined in the Data Protection Framework Directive (Art. 2 a).

The Convention of the Council of Europe on Cybercrime, assigning “traffic data” to a specific legal regime, defines it as “any computer data relating to a communication by means of a computer system, generated

by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service" (Art. 1 d). This definition lists exhaustively the categories of traffic data that is treated by a specific regime in this convention (Explanatory Report, 30). The basic idea of this definition is that traffic data is data used by the telecommunications service providers to allow them to supervise the network. This type of data does not need to be personal [33].

In United States law (Stored Communications Act), "transactional" data lists certain customer record information: the customers name, address, phone numbers, billing records, and types of services the customer utilizes. The USA PATRIOT Act (2001) expanded this list to include "records of session times and durations," any temporarily assigned network address, and "any credit card or bank account number" used for payment [43,34].

### **20.2.2 Interception, Preservation, and Retention**

Traditionally, the interception and collection of content data (i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication) has been a useful tool for law enforcement authorities. Telecommunications interception is defined as a third party acquiring knowledge of the content and/or data relating to private telecommunications between two or more correspondents and, in particular, of traffic data concerning the use of telecommunications activities [2]. American courts have uniformly concluded that an interception of an electronic communication occurs only when the communication is seized during its transmission and before it becomes available to the subscriber [7].

Highly important for law enforcement purposes is to further the measures of data preservation and data retention. As underlined in the Explanatory Report of the Cybercrime Convention of the Council of Europe, traffic data might last only ephemerally, which would make it necessary to order its expeditious preservation. In the language of the Cybercrime Convention, data preservation is the procedure of keeping stored data secure and safe. "Data preservation" must be distinguished from "data retention." The preservation measures apply also to computer data that "has been stored by means of a computer system," which presupposes that the data already exists, has already been collected, and is stored. Expedited data preservation claims, within the framework of a specific investigation or proceeding, the right for the relevant authorities to compel a provider (already in possession of certain data on a specific subscriber/user) to conserve it against the possibility of disappearing.

The so-called "fast-freeze-quick-thaw" model [5], adopted by the Council of Europe and the United States (1986), targets principally the communications of a specific individual, who is already under investigation. As noted

by Crump, data preservation “demonstrates the utility of Internet traffic data as evidence of criminal wrongdoing;” whether data retention, “by making it easier to link acts to actors,” aims at the change of the communication context [15].

## 20.3 European Regulatory Framework

### 20.3.1 *Cybercrime Convention of the Council of Europe*

The Council of Europe (CoE) adopted, in November 2001, the first international legal text on cyber-crime. The CoE aimed at adapting the substantive and procedural criminal law “to technological developments, which offer highly sophisticated opportunities for misusing facilities of the cyberspace and causing damage to legitimate interests.” Given the cross-border nature of information networks, a “binding international instrument” was deemed necessary in order to “ensure... efficiency in the fight against these new phenomena” [13]. The convention was originally open to the members of the CoE and to countries that were involved in its development like the United States, Canada, Japan, and South Africa and came into force on January 7, 2004, once it was ratified by five signatory states, all of which are members of the CoE.

The convention provides for the criminalization of certain online-conducted activities. Included are offenses against the confidentiality, integrity, and availability of computer data and systems (e.g., unauthorized access, etc.), computer-related fraud and forgery, content-related offenses of unlawful production or distribution of child pornography, and offenses related to infringements of copyright and related rights. The convention sets out procedural powers to be adopted by the signing states: expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data; interception of content data, which will apply to any offense committed by means of a computer system or the evidence of which is in electronic form. The Convention also contains provisions concerning traditional and computer crime-related mutual assistance as well as extradition rules.

Article 16 of the Cybercrime Convention envisages the rapid preservation as being for a maximum, though renewable, term of 90 days. It aims at ensuring that competent national authorities are able to order or similarly obtain the expedited preservation of provisory stored computer data in connection with a specific criminal investigation or proceeding. The convention establishes specific obligations in relation to the preservation of traffic data and provides for expeditious disclosure of some traffic

data so as to identify that other service providers were involved in the transmission of the specified communications.

The measures in Articles 16 and 17 apply to stored data that has already been collected and retained by data holders, such as service providers. They do not apply to the real-time collection and retention of future traffic data or to real-time access to the content of communications. The Convention neither requires nor authorizes the signing States to impose supplementary data conservation obligations upon providers and certainly not to operate such conservation as a general regime for all uses of their services [35]. However, Articles 20 and 21 provide for the real-time collection of traffic data and the real-time interception of content data associated with specified communications transmitted by a computer system.

The first drafts of the convention were strongly criticized, as they initially introduced a general surveillance obligation consisting of the routine retention of all traffic data, an approach abandoned “due to the lack of consensus” [13]. The Art. 29 Data Protection Working Party (DPWP), a committee composed of representatives of supervisory authorities designated by EU Member States (Art. 29 of the Framework Data Protection Directive), had expressed serious concerns regarding the vague and confusing wording of the Convention [3]. However, the DPWP had recognized that the Convention’s preservation model, by contrast to the mandatory, routine data retention, is “entirely adequate for the prevention or prosecution of criminal offenses” [4].

### **20.3.2 Privacy and Electronic Communications Law in the European Union**

#### *20.3.2.1 The E-Privacy Directive: Data Retention as an Option*

While the content of communications has already been recognized as deserving protection under constitutional laws, traffic data because of its sensitivity, was considered as “external elements of communication,” even if it reflected a level of interaction between the individual and the environment that rests on similar grounds like the “message” itself. The provision of the Directive 2002/58/EC on privacy and electronic communications (E-privacy Directive) has led to a big improvement on the principle of confidentiality and anonymity by extending the scope of Art. 5 to include not just the content of the communication, but also the related traffic data. Through the new wording, all traffic data generated during the transmission of a communication should enjoy the same confidentiality as provided for the content communications. Electronic communications providers must not disclose any information on contents or data traffic except for the purposes of telecommunications or where explicit law requires it [33].

According to the directive, traffic data generated in the course of an electronic communication should be erased when it is no longer necessary for the purpose of the transmission of the communication. Exemptions to this principle are limited to a small number of specific purposes, such as billing purposes (Art. 6). A “general obligation concerning data retention and any form of systematic interception” would be “contrary to the proportionality principle” [21]. The vigorous debate about the mandatory retention of traffic data ended in 2002 with a compromise solution: Member states were allowed to adopt legislative measures for the retention of data for a limited period, if these are necessary to safeguard national security, defense, public security, and the prevention, investigation, detection, and prosecution of criminal offenses, etc. (Art. 15 § 1). Such measures were required to be “necessary, appropriate, and proportionate within a democratic society” and, explicitly, “to comply with the general principles of Community law,” e.g., those recognized by the Charter of Fundamental Rights of the EU (right to privacy, protection of personal data, freedom of expression, and communication) as well as with the fundamental rights guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe (ECHR).

Even if this provision was supposed to constitute an exception to the rules established by the E-privacy directive, “the ability of governments to oblige communication providers to store all data of all of their subscribers could hardly be construed as an exception to be narrowly interpreted” [37]. Furthermore, this provision was widely drafted and it was criticized for making “little distinction between the action, which may be taken in response to extreme terrorist activity and more routine criminal behaviour” [38].

#### 20.3.2.2 *Mandatory, Routine Data Retention: The New Directive*

Four years later, the permissive language of the E-privacy directive has been transformed into an obligation on EU Member States. The “Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communication networks and amending Directive 2002/58/EC” (Data Retention Directive) introduced the EU-wide obligation to compel “the providers of publicly available electronic communications services or public communications networks” to retain “certain data, which is generated or processed by them, in order to ensure that “the data is available for the purpose of the investigation, detection, and prosecution of serious crime, as defined by each Member State in its national law (Art. 1).”

The exclusion of—the initially included—“prevention” of crime from the scope of the directive was the fruit of a privacy-enhancing approach of the European Parliament. However, the reference to undetermined “serious

crime” (instead of the initial proposal’s reference to “fight against terrorism and organized crime”) leaves a very wide margin of appreciation [6], allowing extending the scope of measures, which might not have been taken outside the specific context of terrorism [26]. According to DPWP, “serious crime” should be “clearly defined and delineated” in order to comply with the principle of “finality” (purpose limitation) laid down in all relevant data protection legislative texts [6].

Providers are required to retain data necessary to identify and trace the identity of the source and the destination of a communication, the date, time, duration, type of the communication, as well as data necessary to identify the communication equipment and its location. Covered also is data relating to unsuccessful call attempts, if the relevant data is already stored or logged. The directive requires that the providers “retain only such data as is generated or processed in the process of supplying their communications services. . . It is not intended to merge the technology for retaining data. . .” (Recital 23). The directive is applicable to electronic communication services offered via the Internet, but “it does not apply to the content of the communications” (Art. 5). Article 29 DPWP considers that since the content is excluded from the scope of the directive, “specific guarantees should be introduced in order to ensure a stringent, effective distinction between content and traffic data—both for the Internet and for telephony” [5]. If such a distinction is feasible is a highly controversial issue.

By no later than September 15, 2007, EU member states have to adopt legislative measures to ensure that the data retained is provided to the competent national authorities in specific cases and in accordance with national law, while member states are allowed to postpone until March 15, 2009, the application of the directive to Internet access, Internet telephony, and Internet e-mail. National legislators have to specify the procedures to be followed and the conditions to be fulfilled in order to gain access to retained data “in accordance with necessity and proportionality requirements”(Art. 4). These requirements have to be taken into account especially for the designation of law enforcement authorities, who will have access to the retained data.

With regard to the retention period, the directive requires member states to ensure the data is retained for a minimum of six months and a maximum of two years from the date of the communication (Art. 6). Member states facing “particular circumstances” are allowed to extend the maximum retention period, provided that the commission approves the national measures that deviate from the directive’s provision (Art. 12), a possibility that raises significant concerns relating to the harmonized application [48,28] and mainly to the power afforded to a community institution lacking democratic legitimization.

### 20.3.3 *Data Retention as Interference with the Right to the Respect of (Communicational) Privacy*

Communications data retention interferes with the right to confidential communications guaranteed to individuals by Art. 8 of the European Convention on Human Rights (ECHR), which states that “everyone has the right to respect for his private and family life, his home, and his correspondence.” The convention establishes basic rules regarding fundamental rights and liberties that are applicable throughout the contracting states. According to Art. 6 (2) of the Treaty on European Union, the ECHR is binding not only for member states, but also for the European Union as well. The right to the protection of privacy is recognized also by Art. 7 of the Charter of Fundamental Rights of the European Union.

The notion of privacy could be defined as freedom of unwarranted and arbitrary interference from public authorities or private actors/bodies into activities that society recognizes as belonging to the realm of individual autonomy (private sphere) [23]. The European approach to privacy is largely grounded to the dignity of the person, who operates in self-determination as a member of a free society. (German Federal Constitutional Court, *Census case*, 1983). Dignity as related to privacy is a concept summarizing principles, such as protection of individual’s personality, noncommodification of the individual, noninterference with other’s life choices, and the possibility to act autonomously and freely in society [36,16].

The European Court of Human Rights has not viewed privacy only as a condition of “total secrecy” and/or “separateness.” On the contrary, the court has clearly interpreted the reference to “private life” expansively. In its jurisprudence, the court admitted that the scope of Art. 8 extends to the right of the individual “to establish and develop relationships with other human beings” (Court of Human Rights, *P.G. v. United Kingdom, Niemitz v. Germany*). The Court considers the mere storing of personal information as an interference with the right of privacy, whether or not the state subsequently uses the data against the individual (Court of Human Rights, *Amann v. Switzerland*). Even “public information (i.e., public available information about an individual) can fall within the scope of private life where it is systematically collected and stored by public authorities” (Court of Human Rights, *Rotaru v. Romania*).

The communication with others as well as the use of communication services falls within the zone of (communicational) privacy [14]. In the case *Malone v. UK*, the court asserted that traffic data is an “integral element on the communications made” by telephone. Therefore, the metering (use of a device that registers automatically the numbers dialed, time, and duration) of traffic data without the consent of the subscriber constitutes an interference with Art. 8 [12]. Traffic data retention, as laid down by the Data Retention Directive, interferes with the fundamental right to confidential

communications [5]. The fact that the data is retained by private parties (providers) is not decisive. Significant for the classification as interference, it remains that the authorities have the right, as specified by domestic law, to access the data at any time [8,28].

## 20.4 Privacy and Electronic Communications Law in the United States

### 20.4.1 *The Legal Framework: The Electronic Communications Privacy Act*

Electronic surveillance in the United States emerged as early as the use of telegraph during the Civil War, with Congress attempting to obtain telegraph messages maintained by Western Union; an attempt that raised “quite an outcry” [43]. The current framework of communications surveillance is dominated by the “strong sense of vulnerability” to the terrorist threat. The latter reinforced the orientation of the government to strengthen the hand of law enforcement agencies, enabling them to trace electronic communications. The USA PATRIOT Act emerged as a response to the September 11 attacks, but undoubtedly the significant problems concerning communications surveillance and intelligence gathering predate the recently adopted framework.

Electronic surveillance law is comprised of the statutory regimes introduced by the Electronic Communications Privacy Act (ECPA) of 1986. Congress amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 in order to extend the prohibitions on interception to electronic communications and to craft new guarantees for stored communications and records. ECPA covers wire, oral, and electronic communications and is structured into three titles: (1) the Wiretap Act, (2) the Stored Communications Act, and (3) the Pen Register Act.

The Wiretap Act deals with the interception of communications while in transmission, “even if they are briefly stored” (U.S. Courts of Appeals, *U.S. v. Councilman*). Law enforcement agencies are required to obtain a “warrant-like order,” e.g., a special and specific order issued by a judge on probable cause. The Wiretap Act extended the scope of protection to the in-transit interception of wireless voice communications and to nonvoice electronic communications (e-mail, etc.).

The Stored Communications Act governs communications in “electronic storage,” e.g., any temporary intermediate storage... incidental to the electronic transmission thereof, as well as any storage... for purposes of backup protection. It also allows law enforcement agencies—by merely demonstrating relevance to an ongoing criminal investigation and issuing a subpoena to the Internet service provider (ISP)—to access

subscriber-identifying information, transactional data, and the content of electronic communications that are maintained either incident to transmission or stored in the account.

The Pen Register Act regulates the government's use of pen registers and trap and trace devices, which create lists of one's outgoing and incoming phone calls. A pen register is a device that records the numbers of one's outgoing phone calls (numbers, date, time, and duration). The Patriot Act amended the definition of pen register to include information on e-mails and IP addresses [43,7]. The court must issue an order permitting the installation of such a register based upon a certification of the government office that the information likely to be obtained is relevant to an ongoing criminal investigation [34].

All three statutes generally prohibit unauthorized interception and/or access to communications and information, and provide for prospective and retrospective surveillance, permitting specified exceptions [34]. Preliminarily, it is interesting to note that, although President George Bush encouraged the president of the European Commission to "[r]evis[e] draft privacy directives that call for mandatory destruction to permit the retention of critical data for a reasonable period" (Letter of January 16, 2001), U.S. statutory provisions permit data retention only in respect to specific investigations that are already underway.

#### **20.4.2 The Fourth Amendment and the "(Un)reasonable" Expectation of Communicational Privacy**

The legal array relating to the surveillance of electronic communications has been adopted "against a backdrop of constitutional uncertainty" [7]. In the United States there is no express right to privacy embedded in the Constitution and—with the exception of several highly specific regulations (as ECPA, the Genetic Privacy Act, or the Video Privacy Act)—there is no comprehensive legal framework providing for the protection of privacy. However, in certain situations, the Supreme Court has interpreted the Constitution to protect the privacy of the individuals: In the 1960s and 1970s, the Court reasoned that the Constitution protected a "zone of privacy" that safeguarded individual autonomy in making certain decisions, traditionally left to individual choice, such as whether to have children (Supreme Court, *Row v. Wade*). In *Whalen v. Roe* (1977), the Court held that the zone of privacy extends to the independence in making certain kinds of decision and the individual interest in avoiding disclosure of personal matters. Several U.S. scholars have maintained that privacy is a form of freedom built into social structure and—subsequently—inadequate protection of privacy threatens deliberative democracy by inhibiting people from engaging in democratic activities [44,40,47].

The critical constitutional framework for communicational privacy consists of the Fourth Amendment and its interpretation by the courts, mainly the U.S. Supreme Court. The Fourth Amendment affirms the right of the people to be secure in their persons, homes, papers, and effects, against unreasonable searches and seizure. It generally prohibits searches or seizures without a warrant. A first important issue concerns the notion of search for Fourth Amendment purposes in relation to the framing question, whether a subscriber/person has a “reasonable expectation of privacy” in data transmitted and retained by providers.

In *Katz v. U.S.* (1967), the “lodestar” of Supreme Court surveillance cases, Justice Harlan articulated the two-part requirement for a government action to be considered a search: “First, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable’.” In *Katz*, the Supreme Court decided that an electronic eavesdropping device, commonly referred to as a “wiretap,” placed on the outside of a public phone booth to detect the contents of the phone conversation implicated the Fourth Amendment and was presumptively unreasonable without a warrant. Departing from its previous narrow definition of a search, the Court stated that protected are “people, not places.” According to the Court, also protected are “communications, which the individual seeks to protect as private, even in an area accessible to the public.”

However, since the end of the Warren Court era (1969), the Supreme Court, generating exceptions and exclusions, has interpreted the Fourth Amendment in a way that leaves communications surveillance largely free from constitutional restrictions [24,39]. Twelve years after *Katz*, in *Smith v. Maryland* (1979), the Court reasoned that there is no Fourth Amendment interest in the telephone numbers one dials: A first argument, set out already in another famous case (*United States v. Miller*), concerns the “nonprivate” character of data retained: A person has no reasonable expectation of privacy in information voluntarily revealed to a third party and conveyed by it to a public authority, “even if the information is revealed on the assumption that it will be used only for a limited purpose.” Since people “know that they must convey numerical information to the phone company” and that the phone company records this information for billing purposes, people cannot “harbour any general expectation that the numbers they dial will remain secret” (*Smith v. Maryland*). The underlying principle is that technological possibilities determine the reasonableness of privacy expectations. Furthermore, the Supreme Court subdivides a technologically enhanced communication into content and other parts, which are not protected under the Fourth Amendment: “[A] pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the contents of communications... These devices do not hear sound...” [24,44,39].

One particularly insidious characteristic of the reasonable expectation of privacy approach is that the more individuals rely on technology, the more government intrusion into personal information seems “reasonable.” “If we remain isolated in our homes, with the curtains tightly drawn, the phone and the computer unplugged, we are within the core of Fourth Amendment protection” [10]. It is highly questionable if the Fourth Amendment and the statutory provisions, as currently interpreted, continue to be an adequate regulatory tool for privacy protection in the Internet space and era.

## 20.5 New Challenges, Old Instruments: The Shortcoming of “Content-Envelope” Distinction

By adapting “traditional” procedural requirements to new technological environments, a critical question concerns the terms used to define and regulate the communications surveillance. The choice of “appropriate terminology” has profound impacts on the extent of power granted to state authorities and respectively on the level of protection afforded to citizens. By failing to provide specific definitions or guidance, the law could lead to major interpretation problems relating to the provisions, guarantees, and checks applied, leaving the public authorities a wide discretion to opt for the convenient legal instrument [42]. This remark, among others, refers to the notion of search and seizure, to the differences of transmission and storage, but mainly it concerns the basis distinction of “content” and “traffic/transactional” data.

Both the European and the American regulatory approaches rely on the traditional distinction of “content” and “envelope.” While recognizing that both types of data may have associated privacy interests, the dominant assumption, explicitly or implicitly shared by legislators and courts, is that the privacy interests in respect to content data are greater due to the nature of the communication content or message [13]. However, in the modern network environment, this separation is not quite as obvious. Moreover this distinction does not reflect necessarily a distinction between “sensitive” and “innocuous” information [43].

### 20.5.1 *The Blurring Lines of “Content” and “Envelope”*

Whereas in the context of traditional telephone communications it is quite easy to distinguish dialing, routing, signaling, or billing information and content, in the landscape of electronic communications the frontiers are blurring. There are numerous network services that cannot easily be categorized in a mere distinction between content and traffic data. The ambiguity of separation is particularly acute in the context of the Internet. It is highly uncertain whether e-mail, instant messaging, and other online activities analogous to “speaking” could be covered by the traditional concepts.

E-mail messages contain information sequences that include both address and content [42]. An e-mail's subject line and the name of the file attached (e.g., "Communist manifesto.doc" or "BinLaden. doc") are also arguably content [15].

Content and traffic data are often generated simultaneously. A fundamental question relates to the nature of URLs: even in the basic level a domain name (such as *www.aegean.edu* or *www.aryan-nations.org*) provides information on the content of what the user will find on the Web page [19,7]. In the case of a request operated with a search engine, such as Google or Altavista, a result like *http://www.google.com/sites/web?q=aids+medical+treatment* reveals not only data necessary for the conveyance of an electronic communication, but also elements of content, indicating at least the interests of the user [12], and information that is automatically logged together with the IP address of the user and the time of the search [28].

### 20.5.2 A False Distinction?

Apart from the difficulties of establishing clear distinctions between content and traffic data, it is disputable if—under the changing technological circumstances—the surveillance of content remains more privacy invasive than the retention of/and access to traffic data. It is argued that "the information value and usability of traffic data is extremely high and at least equals that of content," as this data can be analyzed automatically, combined with other data, searched for specific patterns, and sorted according to certain criteria [8].

Justice Stewart, dissenting in *Smith v. United States*, expressed the opinion that "even the phone numbers one dials have some content, in that a list of the phone numbers a person dials easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life." The German Federal Constitutional Court in the "Connection Capture" decision, the German equivalent of American "pen registers," found that also protected are the "specific circumstances of the telecommunications relationship," including "the fact that a call has been attempted" [39]. Privacy relevant can be proved also location information generated by mobile communications infrastructure [32].

The distinction between traffic/transactional data and content becomes more difficult in the case of communications over the Internet, as the latter relies on "packet switching": To obtain e-mail addresses and session times, providers and law enforcement officers have to separate the address from the content of the message [42]. Moreover, even the "to" and "from" lines of an e-mail can be classified as traffic data as they provide more information than a phone number; they, in general, tend to be more person-specific than phone numbers or they may also have other affiliations, such as an employer in the domain name [15,19].

Technological changes transform rapidly the parameters of the distinction of content and external communication elements: Voice over Internet Protocol (VoIP), relying on Internet's packet-switched network, creates the potential for telephone conversations to be trivially stored by the parties involved as well as at the network level [7]. The imminent growth of VoIP is likely to have profound implications on the content-traffic data approach. Such a routine storage would result in the restriction of user's privacy protection, especially where the access to stored data and communications requires less procedural and substantial guarantees as the interception of content. As Swire [46] points out, the spread of VoIP and pervasive caching of telephone communications could create a *reductio ad absurdum* (reduction to absurdity), in which the "reasonable expectation of privacy" would concern "only a few telephone calls that do not happen to be stored anywhere" [46]. This last remark relates to a major challenge, which lawmakers and courts have to meet in the information era, which is to keep pace with the advance of surveillance technologies, practices, and purposes of the—respectively changing—societal needs and expectations.

## 20.6 Data Retention versus Fundamental Freedoms

Given the expanding use of the Internet and the creation of a new (cyber) "space," individuals have a both subjectively and objectively reasonable expectation of privacy and a claim to control the acquisition or release of personal information, which statutes such as ECPA or the Data Retention Directive fail to reflect, let alone to protect. Quite the reverse. Their—mostly vaguely formulated—provisions constitute a threat to the right to privacy. The new communication surveillance measures, adopted both in the European Union and in the United States, have been strongly criticized by parliamentarians, academics, and privacy advocates. Criticism in Europe has put strong emphasis on the disproportionality of measures adopted in relation to the rights and liberties affected [8,38], while in the United States, the criticism has been largely focused on inadequate and insufficient judicial oversight of communication surveillance procedures and measures, partly as a result of the restrictive approach to "reasonable expectation of privacy" [43,24].

### 20.6.1 *An Unnecessary and Disproportionate Measure*

#### 20.6.1.1 *Criteria of "Acceptable" Interference*

According to the ECHR, communications surveillance is unacceptable, unless it fulfills three fundamental criteria set in Art. 8 (2): (1) a legal basis, (2) the need/necessity of the measure in a democratic society, and (3) the

conformity of the measure with the legitimate interests of national security, public safety, or the economic well-being of a country, prevention or disorder of crime, protection of health or morals, or protection of the rights and freedoms of the others. The provision reflects the tension between individual and community and the need to take into account the interests of society without infringing upon the intrinsic value of privacy in a democratic society.

The catalog of justified restrictions on the right to privacy seems to be extensively large. However, the European Court of Human Rights in its case law has specified the requirements to be met. The law authorizing the interference in the communicational privacy has to meet the standards of accessibility and foreseeability inherent in the concept of the rule of law, so that persons can regulate their conduct according to the law (Court of Human Rights, *Malone v. U.K.*, *Kruslin v. France*). Conditions, safeguards for the individuals, and implementation modalities must be sufficiently summarized, in order to succeed the “quality of law” test [12,15].

Proportionality, a key principle in European constitutional law, requires a further assessment of the necessity of the measure and its suitability to achieve its aims. Even if “necessary is not synonymous with indispensable. . . it implies a pressing social need” (Court of Human Rights, *Handyside v. U.K.*). The objective pursued must be balanced against the seriousness of the interference, which is to be judged taking into account, inter alia, the number and nature of persons affected and the intensiveness of the negative effects [8]. Restrictions must be limited to a strict minimum: Legislators are required to minimize the interference by trying to achieve their aims in the least onerous way (Court of Human Rights, *Hatton v. U.K.*). The necessity and proportionality have to be clearly demonstrated by considering that privacy is not only an individual right of control over one’s information, but moreover a key element of a democratic constitutional order (German Constitutional Court, *Census Decision*).

#### 20.6.1.2 A Disproportionate “Dataveillance”

Considerable doubts are expressed about whether the above-mentioned criteria are fulfilled in the EU Data Retention Directive. A first significant objection concerned the necessity of the general data retention. The new framework was adopted without demonstrating that “the (pre)existing legal framework does not offer the instruments that are needed to protect physical security” [20] and this large-scale surveillance potential was the only feasible option for combating crime. Serious concerns have been expressed about the proportionality of means, ends, and—provable—security gains. According to a research of T-Online (a big German provider), only 0.0004% of traffic data retained is needed for law enforcement purposes [9]. However, this framework will apply to all persons who use

European-based electronic communications. The comprehensive storage of all traffic data gives rise to an indefinite and ongoing interference with the privacy rights of all users, not just those who are suspected of committing a crime [14,12,18]. It makes surveillance that is authorized in exceptional circumstances, the “rule” [5]. Additionally, generalized data retention conflicts with the proportionality, fair use, and specificity requirements of data protection regulation: Personal data may not be collected, processed, or transmitted with the sole purpose of providing a future speculative data resource. The adoption of such an invasive measure could result in opening a Pandora’s box of universal surveillance, where every person is treated as a potential criminal [33].

The generalized storing of communication/traffic data is wildly disproportionate to the law enforcement objectives and, therefore, could not be deemed as necessary in a democratic society. Routine retention of traffic and location data concerning all kinds of communications (i.e., mobile phones, SMS, faxes, e-mails, chatrooms, and other uses of the Internet) for purposes varying from national security to law enforcement constitutes what Clarke [11] refers to as “dataveillance,” i.e., the routine, systematic, and focused use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons. Considering the increased use of electronic communications in daily life and the fact that, especially, the Internet is unprecedented in the degree of information that can be stored and revealed, the storage of this data could be seen as an “extended logbook” of a person’s behavior and life [12]. Encroaching into the daily life of every person, routine data retention “may endanger the fundamental values and freedoms that all (European) citizens enjoy and cherish” [6].

### **20.6.2 *Communications Surveillance as Interference into the Rights of Anonymity and Freedom of Expression***

The feature of the electronic communication networks and the interactive use of networks increase the amount of transactional/traffic data generated [1]. As electronic communications leave a lot of “digital traces,” communication surveillance impedes or even eliminates the right to anonymity [43,15]. The ability to maintain one’s anonymity in certain contexts, as in using technology without having to reveal one’s name forms part of privacy [10]. Anonymity has to be assessed not only as a component of private sphere and intimacy, but also and mainly in the context of its significance for the right to freedom of expression, which includes “the right to receive and impart information and ideas without interference by public authorities” (Art. 10 of the European Convention of Human Rights).

According to the landmark decision of the German Federal Constitutional Court on the census law, unrestricted access to personal data imperils

virtually every constitutionally guaranteed right: Neither freedom of speech nor freedom of association nor freedom of assembly can be fully exercised as long as it remains uncertain whether, under what circumstances, and for what purposes, personal information is collected and processed. Blanket data retention, by making communication activity potentially traceable, has a disturbing effect on the willingness to voice critical and constructive ideas, and on the free exchange of information and ideas, which is of paramount importance in a democratic society [8,29]. Identification and fear of reprisal might discourage participation to public debate (U.S. Supreme Court, *Talley v. California*). On the contrary, anonymity allows information and ideas to be disseminated and considered without bias. The U.S. Supreme Court has found that the Constitution protects the right to receive information and ideas and, more specifically, that the First Amendment extends to anonymous speech activity.

The claim to anonymity, inherent in the right to privacy, is essential to freedom of communication via electronic networks, but, at the same time, it runs against public policy objectives. From a law enforcement perspective, anonymity is perceived as the main reason for increasing cyber-criminal activity [12]. However, there is no sustainable argument for abandoning the principle that where a choice of offline anonymity exists, it should also be preserved in the online world (*Ministerial Declaration of the Ministerial Conference on Global Information Networks*, Bonn, 1997). Proportionate restrictions to this right, in order to face the specific nature and risks of cyberspace activities, must be permitted in limited and specified circumstances. The Supreme Court, acknowledging the instrumental value of anonymity in enriching public discussion and maximizing freedom of (anonymous) association [15], has held that this constitutionally guaranteed right must be reconciled with compelling public interests. According to the Court, identification is held to be constitutional only if there is no other effective way for the government to achieve law enforcement objectives (*Buckley v. Valeo*).

### **20.6.3 The Question of Independent and Adequate Oversight**

As a counterpart to restrictions of freedoms that governments adopt to respond to public security threats, adequate safeguards and remedies must be provided that can counter possible abuse by the administration and specifically by the law enforcement authorities [22]. The involvement of independent oversight mechanisms is a crucial element in order to ensure the lawful access to communications data and records and guarantee that the consequences for individuals and their rights and freedoms are limited to the strict minimum necessary.

Following the opinion of the DPWP, access to data, in principle, should be duly authorized by a judicial authority, who, where appropriate, should

specify the particular data required for the specific cases at hand. Effective controls on the original and any further use should be provided: (1) by judicial authorities within and for the purposes of a criminal procedure and (2) by data protection authorities concerning data protection, regardless of the existence of a judicial proceeding [5,6]. Independent supervisory authorities have become an essential component of the data protection supervisory system in the EU. The Data Retention Directive requires member states to designate one or more public authorities, acting with complete independence. However, in this case, the EU legislators have a narrow perception of their competence, as it seems to be restricted to “monitoring the application of the national law provisions adopted by Member States regarding the security of the stored data” (Art. 9).

In the United States, the Wiretap Act requires the government to meet very high standards in order to obtain authorization to intercept communications (specific description, type, duration, etc.). However, the most significant deficiency is that the majority of the statutes permits governmental access to third-party records with only a court order or subpoena, which falls short of the Fourth Amendment’s requirement for warrants supported by probable cause and issued by a neutral and detached judge. Regular warrants are required only to obtain the contents of electronic communications in electronic storage for 180 days or less. If they are stored over 180 days, the government can access them with an administrative subpoena, a grand jury subpoena, a trial subpoena, or a court order. In the case of the Pen Registers Act, the courts must take the government’s certification that the information is relevant to an ongoing investigation. Judges are not required to review the evidence and assess the factual predicate for the government’s certification. Several scholars have stressed the need for a higher threshold to obtain the court order and for the guarantee of judicial review of the government’s application [43]. Another point of criticism has been the fact that the ECPA contains no statutory exclusionary rule for wrongfully acquired electronic communications, which means that it does not prohibit the use as evidence of any communications obtained in violation of these requirements [7].

#### **20.6.4 Common Information Pools for Public and Private Sector**

Systematic data retention is a paradigm for (recently enhanced) policies, which aim at enabling and promoting increased data sharing between the public and the private domain, particularly for prevention and law enforcement purposes. The exploding collection of consumer information by private sector actors has produced enormous pools of information, which can be adapted to domestic surveillance [44,29]. Especially in the aftermath of September 11, data flows (increasingly and often internationally) from

the private sector, ranging from banks and insurances (SWIFT case, Choice-Point case) to airlines (EU–USA PNR data case), to governmental agencies. Privatization and diversification of traditionally state-controlled sectors (like telecommunications), interoperability, and technological synergy have as consequence the so-called “function creep,” which can result in a “mission creep” [37]. “For example, not only are the same data-mining techniques developed for profiling consumers being used by security and intelligence services to profile potential terrorists, often the very data from which these profiles are created is the same” [45].

Regardless, the national rules being developed to regulate access to traffic data by law enforcement agencies, will mean that mandatory retention would effectively create a massive database, putting at the disposal of the state an unprecedented amount of information about the everyday activities of—indiscriminately—each and every user. The increasing amount of personal information flowing to the government poses significant problems with far-reaching effects [44]. The (even potential) availability and accessibility of vast amounts of data, collected by private entities for entirely other purposes, constitutes a threat to informational self-determination and it can chill not only politics-related, but also personal activities.

## 20.7 An Information-Based (Pre)prevention of Risks or a Threat to Democracy

The terrorist attacks in the United States, Europe, and elsewhere, and the expansion of organized crime/cyber-crime, have altered the balance of security interests and freedom in a way that deeply affects the fundamental values, which form the basis of democratic and constitutional states. Surveillance-susceptible infrastructures and data-retention schemes supply the governments with new privacy-intrusive surveillance tools. As life in the information society depends upon information and communication, data retention extends beyond a potential search basis: Not only does “it rigidifies one’s past” [43], but it records citizen’s behavior and social interaction [34,8]. Pervasive surveillance affects the self-determination and the personality of individuals, inclining their choices toward the mainstream [41,43]. “Potential knowledge is present power,” emphasizes the Report of the [U.S. Department of Defense] Technology and Privacy Advisory Committee, adding, “awareness that government may analyze activity is likely to alter behavior” as “people act differently if they know their conduct could be observed” [49]. Data retention symbolizes the “disappearance of the disappearance,” which seems to become a defining characteristic of the information age [31]. In this sense, the “freedom of movement,” another historically fundamental freedom right, is currently jeopardized in virtual “spaces.”

The decision to routinely retain communications data for law enforcement purposes is “an unprecedented one with a historical dimension” [6]. It reflects the transformation from the traditional constitutional model of gathering conclusive evidence of wrongdoing of suspect individuals toward intelligence gathering, which may be carried out against individuals at random [31,17]. The individual itself “is no longer perceived as a principally law-abiding citizen, rather as a potential threat” or “as an exchangeable element in a principally dangerous environment” [30]. Further, even after the deletion of “prevention” from the aims allowing access to retained data according to EU law, generalized, and indiscriminate data retention, as such, mirrors the shift from a constitutional state guarding against the threat of specific risks in specific situations toward a security-orientated preventive [17] or even prepreventive state, which acts operatively and proactively. The imperative to fight new threats through preprevention measures and policies “blows up the cornerstones of the rule of law state” [25].

The rapid reaction to the expectation of the people that the government will keep the “security promise,” reveals certainly the state’s readiness to suspend freedom [26], merely catalyzed, yet not caused, by the latest terrorist acts. The “invention” of a “fundamental right to security” did nothing to resolve the problems of security, but was only used as an argument to justify everwider powers of state intervention [17,26]. Prevention and removal of risks have become a social and political imperative in the risk society. Curtailment of rights and reduction of scrutiny seems to be in large extent tolerated by majorities [15]. A decisive question is if and to what extent the society is ready to take risks in freedom’s interest.

Governments must respond to the new challenge in a way that effectively meets the citizens’ expectations without undermining individual human rights “or even destroying democracy on the ground of defending it” (European Court, *Klass v. Germany*). Absolute security could not exist because it could be achieved only at the price of freedom. The legitimization of the democratic state depends upon its success in balancing the various public objectives, i.e., freedom and security, under the terms and within the limits of core democratic values. Levi and Wall [31] propose as “guidance for future directions or thoughts” Benjamin Franklin’s famous quote: “Any society that would give up a little liberty to gain a little security will deserve neither and lose both.”

## References

- [1] Article 29, Data Protection Working Party, Recommendation 3/97 Anonymity on the Internet, December 1997.
- [2] Article 29, Data Protection Working Party, Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications, May 1999.

- [3] Article 29, Data Protection Working Party, Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-Crime, March 2001.
- [4] Article 29, Data Protection Working Party, Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communication networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism, November 2004.
- [5] Article 29, Data Protection Working Party, Opinion 113/2005 on the Proposal for a Directive on the retention of data processed in connection with the Provision of Public Electronic Communication services and amending Directive 2002/58/EC, October 2005.
- [6] Article 29, Data Protection Working Party, Opinion 3/2006 on the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC, March 2006.
- [7] Bellia, P.L., The Fourth Amendment and Emerging Communications Technologies, *IEEE Security and Privacy*, 20, 2006.
- [8] Breyer, P., Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, *European Law Journal*, 11, 365, 2005.
- [9] Breyer, P., Bürgerrechte und TKG-Novelle—Datenschutzrechtliche Auswirkungen der Neufassung des Telekommunikationsgesetzes, *Recht der Datenverarbeitung*, 20, 147, 2004.
- [10] Cheh, M., Technology and privacy: creating the conditions for preserving personal privacy, in *Scientific and Technological Developments and Human Rights*, Sicilianos, L.A. and Gavouneli, M., Eds., Ant. Sakkoulas Publishers, Athens, 2001, 99.
- [11] Clark, R., Introduction to dataveillance and information privacy [2006 (1997)]: <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro#DV>
- [12] Coemans, C. and Dumortier, J., Enforcement issues—Mandatory retention of traffic data in the EU: Possible impact on privacy and on-line anonymity, in *Digital Anonymity and the Law*, Nicoll, C. Prince J.E.J., and van Dellen, J.M., Eds., TMC Asser Press, The Hague, the Netherlands, 2003, 161.
- [13] Council of Europe, Convention on Cybercrime—Explanatory report, 2001.
- [14] Covington and Burling LLP, Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights, Memorandum prepared for Privacy International (October 10, 2003): <http://www.privacyinternational.org/issues/terrorism/>
- [15] Crump, C., Data retention—Privacy, anonymity, and accountability online, *Stanford Law Review*, 56, 191, 2003.
- [16] De Hert, P. Balancing security and liberty within the European Human Rights Framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11, *Utrecht Law Review*, 1, 68, 2005.

- [17] Denninger, E., Freiheit durch Sicherheit? Wie viel Schutz der inneren Sicherheit verlangt und verträgt das deutsche Grundgesetz?, *Kritische Justiz*, 35, 467, 2002.
- [18] Deutscher Bundestag–Wissenschaftliche Dienste (Sierck, G., Schöning, F., and Pöhl, M.), *Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht—Ausarbeitung*, Berlin, 2006.
- [19] Ditzion, R., Electronic surveillance in the Internet age: The strange case of Pen Registers, *American Criminal Law Review*, 41, 1321, 2004.
- [20] European Data Protection Supervisor, Opinion on the Proposal for a Directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC.
- [21] European Parliament, Recommendation on the strategy for creating a safer information society by improving the security of information infrastructures and combating computer-related crime, C 72 E/323-329 *Official Journal of EC*, March 31, 2002.
- [22] EU Network of Independent Experts in Fundamental Rights—CRF-DF, Comment, *The Balance between Freedom and Security in the Response by the EU and Its MS to the Terrorist Threat*, 2003.
- [23] EU Network of Independent Experts on Fundamental Rights—CRF-DF, Commentary of the Charter of Fundamental Rights of the European Union, June 2006.
- [24] Herman, S.N., The USA PATRIOT Act and the submajoritarian Fourth Amendment, *Harvard Civil Rights–Civil Liberties Law Review*, 41, 67, 2006.
- [25] Hoffmann-Riem, W., Freiheit und Sicherheit im Angesicht terroristischer Anschläge, *Zeitschrift für Rechtspolitik*, 35, 497, 2002.
- [26] Hustinx, P.J. (European Data Protection Supervisor), Human rights and public security: Chance for a compromise or continuity of safeguards? in *Conference on Public Security and Data Protection*, Warsaw, 2006.
- [27] Institute For Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*: Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs, European Communities, 2003.
- [28] Kosta, E. and Valcke, P., Retaining the data retention directive, *Computer Law & Security Report*, 22, 370, 2006.
- [29] Kreimer, S.F., Watching the watchers: Surveillance, transparency and political freedom in the war on terror, *University of Pennsylvania Journal of Constitutional Law*, 7, 133, 2004.
- [30] Lepsius, O., Liberty, security and terrorism: The legal position in Germany, Part 2, *German Law Journal*, 5, 435, 2004.
- [31] Levi, M. and Wall, D.S., Technologies, security and privacy in the Post-9/11 European Information Society, *Journal of Law and Society*, 31, 194, 2004.
- [32] McPhie, D., Almost private: Pen registers, packet sniffers, and privacy at the margin, *Stanford Technology Law Review*, 1, 2005.
- [33] Mitrou, E. and Moulinos, K., Privacy and Data Protection in Electronic Communications, in *Proc. Int. Workshop Computer Network Security*, Gorodetsky, V., Popyack, L., and Skormin, V., Eds., Springer, Berlin-Heidelberg, 2003, 432.

- [34] Mulligan, D.K., Reasonable expectations in electronic communications: A critical perspective on the Electronic Communications Privacy Act, *George Washington Law Review*, 72, 1557, 2004.
- [35] Poulet, Y., The fight against crime and/or the protection of privacy: A thorny debate, *International Review of Law Computers & Technology*, 18, 251, 2004.
- [36] Rodota, S., Privacy, freedom and dignity, closing remarks at the 26th *International Conference on Privacy and Personal Data Protection*, Wrocław, Poland, September 16, 2004.
- [37] Rotenberg, M. et al. Privacy and human rights 2005—An international survey of privacy laws and developments, Electronic Privacy Information Center, Privacy International, <http://www.privacyinternational.org/index/> September 7, 2006.
- [38] Rowland, D., Data retention and the war against terrorism—A considered and proportionate response? *The Journal of Information, Law and Technology*, (3) 2004, [www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004\\_3/](http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_3/)
- [39] Schwartz, P.M., German and U.S. telecommunications privacy law: Legal regulation of domestic law enforcement surveillance, *Hastings Law Journal*, 54, 751, 2003.
- [40] Schwartz, P.M. and Reidenberg, J.R., *Data Privacy Law—A Study of United States Data Protection*, Michie Law Publishers, Charlottesville, VA, 1996.
- [41] Simitis, S., Reviewing privacy in an Information Society, *University of Pennsylvania Law Review*, 135, 707, 1987.
- [42] Smith, J.C., The USA PATRIOT Act: Violating reasonable expectations of privacy protected by the Fourth Amendment without advancing national security, *North Carolina Law Review*, 82, 412, 2003.
- [43] Solove, D.J., Reconstructing the electronic surveillance law, *The George Washington Law Review*, 72, 1701, 2004.
- [44] Solove, D.J., Digital dossiers and the dissipation of Fourth Amendment Privacy, *Southern California Law Review*, 75, 1084, 2002.
- [45] Surveillance Studies Network (Wood, D.M., Ed.), A report on the Surveillance Society for the (UK) Information Commissioner, September 2006.
- [46] Swire, P.P., Katz is dead. Long live Katz, *Michigan Law Review*, 102, 904, 2004.
- [47] Taipale, K.A., Technology, security and privacy: The fear of Frankenstein, the mythology of privacy and the lessons of King Ludd, *Yale Journal of Law and Technology*, 7, 123, 2004–2005.
- [48] Taylor, M., The EU Data Retention Directive, *Computer Law and Security Report*, 22, 309, 2006.
- [49] U.S. Department of Defense, Report from the Technology and Privacy Advisory Committee Safeguarding Privacy in the Fight Against Terrorism, March 2004, available at <http://www.sainc.com/tapac/finalReport.htm>

P1: Binod

November 16, 2007 12:26 AU5217 AU5217C020