Preface

THE PRIVACY-TECHNOLOGY DILEMMA IN THE AGE OF DIGITAL SURVEILLANCE

The proliferation of new technologies and their increasing use in many aspects of our lives pose a number of threats to privacy; digital networks, ubiquitous computing, ambient intelligence, automated profiling, genetics, radio frequency identification (RFID), wiretapping, closed circuit television (CCTV) cameras, digital rights management systems and similar technologies challenge the traditional confines of privacy, and on several occasions, call for its reconceptualization. In a dynamically changing technological framework one must answer the following dilemma: how to benefit from the friendly uses of technology without surrendering the individual’s freedom and autonomy. The contributions that are included in the book that follows introduce exactly this dilemma, trying to propose possible solutions and answers, policies or practices that can balance the benefits of technology with the need to protect the right to privacy in an era of surveillance and digital technology.

The difficult balance between technology and privacy is a subject that has already drawn the international theoretical attention. Privacy, a relatively new right—at least for many of the European legal orders (e.g. Greece, France, Italy, Germany, Spain, Portugal)—has attracted the European theoretical attention over the past three decades exactly due to the rapid rise of technology. Nonetheless, the things are quite different in the other side of the Atlantic, beginning with the American theoretical dialogue on the subject initiated by the famous ‘right to be left alone’ of S. D. Warren and L. D. Brandeis. In their ‘Right to Privacy’ published in the Harvard Law Review in 1890, the two authors base the necessity for acknowledging an implicit right to privacy exactly in the rise of technology and the new threats that the press casts for the freedom of the individual. In the exact same way, nowadays the network, the data-banks and the technologies of surveillance present new endangerments that call for the protection of privacy.

This very idea connects the chapters in this book. Technology does not only present a possible threat to privacy. It also reflects the very contours of privacy, the reason that its protection becomes a legal and social necessity. This is the reason why the expansion of technology also analogically augments the legal acknowledgment of the social appreciation of privacy. This evolution has influenced the rise of the ‘public safety’ international technological surveillance, the relevant bibliography on the subject of privacy and technology over the past two decades, and especially after the September 11, 2001. Among others, some characteristic approaches are presented in Agre and Rotenberg (1997), Wagner-DeCew (1997), Brin (1998), Friedman (2000), and Austin (2003).

The contributions that follow engage to this open dialogue, by offering new theoretical proposals and mainly a modern taxonomy of privacy-technology problems as well as solutions, proposals and
specific policy models. Thus, the book is divided in six sections, all of them encountering some of the most currently debated subject of the privacy-technology clash.

Section One revisits basic concepts associated with privacy, such as personality and identity, against the background of digital networks that entail potential dangers for privacy. All three chapters of this Section acknowledge the interconnectedness of digital information systems and the pervasiveness of electronic recordkeeping, and suggest alternative ways of viewing privacy and identity in these new environments.

More specifically, Bradley Tennis in Chapter 1 picks up on the idea of a redefinition of privacy in a networked world in view of the evolution of digital information technologies. He observes that traditional distinctions between public and private spheres are not readily applicable to the digital realm. The Internet, he writes, cannot be neatly categorized as either a public or a private space; it is a complex combination of semi-private, potentially overlapping spaces nestled in a public medium. Therefore, traditional regulatory tools prove ill-equipped to protect privacy and identity interests in today’s networked world. Instead, these developments call for the recognition of an individual’s right to control the dissemination of their personal information, and publicly project multiple personae by compartmentalizing different aspects of their online conduct.

The chapter begins by examining how the legal system has adapted to account for the manifestation of familiar information privacy concerns in the examples of anonymous speech and disclosure of personal information. With respect to the former, Tennis points out the danger that civil suits resulting in de-anonymization stifle online speech and cultural production. On the other hand, true victims of online harassment or defamation need to be protected. He argues that the requirements that the plaintiff make a strong showing that his claim is colorable and that the defendant receive notice generally strike an appropriate balance between these two concerns. When it comes to third party disclosure, Tennis suggests that the risk of extensive, detailed dossiers on users of online services being transferred to third parties highlights the need to adopt a uniform and broad definition of “personal information,” strengthen notice and consent provisions, and provide users the opportunity to opt out of the data sharing provisions of a particular service’s privacy policy not necessary to the production of the service. Chapter 1 then goes on to advocate a perception of privacy entailing an individual’s right to publicly project multiple personae while still maintaining boundaries between them. This compartmentalization promotes the realization of and participation in a full democratic culture in that it allows a user to participate in the production of information and culture that might prove damaging or embarrassing if associated with them in other contexts. The chapter last examines potential safeguards for these privacy and identity interests. It concludes that Canadian and EU legislation with their expansive reading of “personal information” and the level of control that an individual should be able to exert over the collection, use, and dissemination of this information provide a step in the right direction.

Chapter 2 continues the inquiry into the concepts of privacy and identity. Norberto Nuno Gomes de Andrade emphasizes the need for a clear demarcation between the two rights. He criticizes overly broad definitions of the right to privacy that claim some of the definitional and constitutive characteristics pertaining to the right to identity. He then assesses the ambiguous and dynamic relationship between privacy and identity, providing examples of how privacy may obstruct identity, and identity may undermine privacy. While both the right to privacy and the right to identity have common roots in the so-called personality rights and relate to an individual’s right to dignity and self-determination, they constitute two different and autonomous rights: the right to identity translates a person’s definite and inalienable interest in the uniqueness of his being, whereas the right to privacy describes a personal condition of life characterized by seclusion from the public.
Building on this distinction the chapter introduces a “privacy-identity relevance” factor into the categorization of personal information. According to what Andrade calls the “alethic criterion” (from the Greek word for truth), the right to identity concerns all those personal facts—regardless of being truthful or not— which are capable of falsifying or transmitting a wrong image of one’s identity, while the right to privacy comprises only those true personal facts that are part of one’s private sphere and which, by one reason or the other, spill over to the public sphere. This distinction has significant implications, the author argues, in the foreseeable scenario of a Ubiquitous Computing world, and more specifically in the case of automated profiling technologies. In this context the application of the right to privacy and the right to identity will depend on the type of profile in question, that is, on whether the profile involves the disclosure of any necessarily true facts related to the subject or not. The right to privacy will play an important role in the first phase of the profiling process (the data phase), regulating the manner in which personal data may be captured, collected and stored. The right to identity shall then play a crucial role in the second phase of the profiling process (the knowledge phase), allowing the individual to gain access and eventually contest on the grounds of misrepresentation the knowledge that has been constructed about him or her through such profiles.

Chapter 3 takes a more skeptical view towards the significance of privacy in the digital era. Konstantinos Stylianou endorses a version of technological determinism, whereby in the name of new technological vistas that maximize access to information privacy folds. He adopts a broad definition of privacy that would include all activity and all information that the subject has a reasonable expectation to keep to himself, the expectation to be free from unwarranted governmental or private intrusion, the option not to become the object of attention, the right to remain anonymous, and the ability to block physical access to himself. However, the author argues that privacy is overrated in a twofold sense: first, the ready availability of a huge volume of personal information creates attention scarcity thus diminishing the chances that a person’s privacy will be intruded. But even when the dangers are real, as an empirical matter people are often willing to compromise their privacy for the benefits a given technology has to offer. For this reason, effective allocation of resources would mandate a shift in emphasis from regulation of collection of data to regulation of use of data. In this context, Stylianou suggests, self-regulation could be an alternative means of regulation worth considering.

The right to privacy faces new threats when it encounters demands for national security and public safety. This is the focus of Section Two of the book. Especially after September 11, there is a shift in emphasis toward fighting terrorist and other criminal activities. These demands for the protection of national and public security often explicitly call for or in practice result in relaxing privacy protections. Both chapters point out that in this environment the private easily becomes of public concern, but they are quick to highlight the dangers associated with such a shift.

Chapter 4 begins this inquiry by critically assessing the practice of video surveillance by means of CCTV systems. Haralambos Anthopoulos argues that a Greek statutory exemption from the data protection legislation for all police activities involving data processing during public assemblies is unconstitutional as it runs counter to the rights to political privacy and public anonymity. He explains that the right to data protection is enshrined in the Greek Constitution and includes within its scope of protection “sensitive data,” such as those related to political views. This heightened protection enhances the freedom of political and social activity of the individual, securing his “political privacy.” In the case of public assemblies, Anthopoulos continues, the right to data protection directly correlates with the constitutionally protected freedom of assembly. By combining the two rights he advocates the creation of a new constitutional rule, according to which participants in lawful open public assemblies and demonstrations have the right not to
be massively identified through the use of video-surveillance systems recording and storing their image, i.e., the “right to public anonymity.” Furthermore, these constitutional provisions do not provide for any exemptions from their application for the sake of public security. Against this constitutional backdrop, the author maintains that the statutory exemption in question raises constitutional issues, especially in that it does not distinguish assemblies into a) lawful open public assemblies, b) open public assemblies where crimes are committed by random passengers or sole participants, and c) unlawful open public assemblies. The Chapter concludes by examining the jurisprudence of the European Court of Human Rights which seems to suggest that a breach of privacy can only be ascertained in the case of further processing of the collected material with the purpose of identification of persons recorded in it or when this information is made publicly available.

Melike Akkaraca Köse continues in this thematic in Chapter 5 by examining a “traditional” form of state surveillance: telecommunication interceptions. The author presents the applicable legal regime and domestic reforms introducing strict legal standards for communications surveillance. She notes that most of the problems regarding privacy occur due to the preventive surveillance of communications which may be applied for the abstractly defined crimes and without a serious ground for suspicion. However, Turkish laws do not show important disparities compared to the other telecommunications surveillance regulations in Europe. Akkaraca explains that, despite the positive legal reforms, the problems lie in the implementation of law by state officials. She then goes on to chronicle a series of wiretaps directed against high-ranked members of the judiciary, politicians and members of the public. The focus is on the “Ergenekon” case in which indictments relied on documents seized at the defendants’ homes and wiretaps; these evidence collection methods have been described as dubious.

To evaluate these practices Chapter 5 employs a Foucauldian approach: the aim is to uncover the “conditions of possibility” for the widespread practice of wiretapping in Turkey by focusing on the actual power relations. According to the author, the surveillance of communications is a technique of discipline in a Foucauldian sense. Turkey’s security conceptions may only be explained by a number of truth-claims developed by different powers in the society. The army is one of them: Akkaraca observes that the frequent use of surveillance techniques by the military is directly linked to the 2009 wiretapping scandal since it exhibits a well-established practice of limitless use of disciplinary techniques against individuals when the ‘security’ is at stake. Another power producing truth-claims about security in Turkey is the judiciary. The problem there lies in the limited approach it adopted in the cases concerning security and human rights. This situation, the author notes, encourages claims about the judiciary-military cooperation. On the other hand, the AKP ruling party produces most of the truth-claims critical toward the judicial and military discourses. The Chapter argues that the Ergenekon case is to be evaluated against this background. The question is whether the case is another stage of the conflicts of power or truly a struggle against the long-persisting stay-behind organizations.

The section is closing by Anna Tsiftsoglou’s Chapter 6 presentation on the clash between data protection and public safety in the framework of the Greek dialogue concerning the legislative acknowledgement (Law 3783/2009) of public surveillance for reasons of preventing crime and protecting public safety. The chapter analyzes both the Greek and EU legislation in comparison as well as it conceptualizes the concept of public safety and the basis of its ‘inherent’ clash to privacy.

Section Three moves the investigation to the area of medical and genetic privacy and the role of medical technology in the relevant debates. The examples discussed in this Section are genetics and abortion. The fact that the “object” of privacy protection in this domain is our own body also invites an ethical approach to these questions, which both chapters in this section adopt.
Christina Akrivopoulou in Chapter 7 examines the right to genetic privacy on the basis of the equilibrium of individual autonomy, family and public interest. She begins by presenting the individualistic aspect of the right noting that a deep knowledge of our genetic self promotes our autonomy. However, it also creates bonds with others since it represents a part of the subject’s family heritage. Our genetic identity, she writes, is crucial for the family intimacy that we enjoy. This differentiates genetic information from any other type of medical information because the former bears a part of our personality, of our identity and autonomy, and is therefore not neutral. It consequently follows that the individual has a private interest in keeping it secure against threats posed by geneticism, genetic exceptionalism and genetic determinism that could provide grounds for unequal, discriminatory, or even outright totalitarian treatment of the individual. This leads to a discussion of the notion of “control” that has been proposed as the best remedy against such risks. Akrivopoulou argues that this notion is premised on a spatial or proprietary understanding of privacy that ignores the shared and ethical character of this right. Similarly, she cautions against the capacity of consent to offer “magic potion” solutions for all the choices connected to the individual’s genetic privacy and freedom. The author then examines the ethical grounds for genetic privacy which she situates in autonomy while also taking into account the dignity and personality of the individual. The implications of grounding this right in autonomy—as opposed to the concept of control—is that it gives rise to the concept of free choice. Furthermore, basing a right to genetic privacy on autonomy and choice precludes the threat of paternalism as it entails the capacity of the subject to make harmful choices against his/her welfare. Last, the Chapter critically examines the liberal and communitarian approaches to genetic privacy in favor of what the author calls “genetic privacy as autonomy of care” that values the individual as well as the intimate relationships in which he/she chooses to participate in the same way, thus enabling his/her communication and formation of choices in a circle of trust instead of an isolated but private and dominant space.

Hasan Atilla Güngör in Chapter 8 focuses on a different aspect of the right to privacy, that related to abortion. He examines how scientific developments have been used both by pro-choice and pro-life groups in support of their cause, and argues that scientific claims concerning the fetus’ ability to feel pain may more appropriately underpin the development of regulations in this area. The chapter begins by assessing the debates between the two groups revolving around scientific arguments about when human life begins. It presents five criteria that were developed over the years to try to answer this question as well as the scientific objections raised against them. The author notes that this scientific debate has not provided conclusive responses but rather seems to have exacerbated disagreements. He then suggests that formulating the question in terms of a clash between the unborn child’s right to life and the woman’s right to privacy is oversimplified and unfair: the reason is that in addition to a woman’s right to privacy, other rights are also implicated, namely her rights to health and life. This does not mean, Güngör continues, that the fetus is left unprotected as it does enjoy private and public law protections. He stresses, however, that according legal personality to the fetus would lead to paradoxes and eliminate women’s rights. What the chapter recommends instead is that each phase through which the fetus passes during the prenatal period be dealt through the invocation of distinctive legal categories. In this context, the author introduces the criterion of whether the fetus can feel pain. He clarifies that this does not suggest that abortion must be banned when the fetus begins to experience the feeling of pain. Rather, this criterion advocates establishing new legal mechanisms aiming to provide the least possible or even no pain for the fetus during its extraction from the mother’s womb.

The section is closing with the contribution of Cristina Contartese in Chapter 9 which aims in presenting the clash between the protection of genetic data and national security in the jurisprudence of
the European Court of Human Rights. By accounting several significant cases of the European Court of Human Rights, including the famous Marper vs the U.K., the author focuses on the importance of protecting the genetic privacy of the individual as well as the possible threats that the relevant technology poses against our control over our personal information.

Section Four addresses another issue of increasing importance nowadays, that of tagging (of humans and objects) and its threats to privacy. The first chapter in this Section discusses the implementation of RFID technology in the hospital setting and the different levels of privacy risks implicated in these applications. The second chapter examines a narrower case of RFID application in the registration of motor vehicles and finds that it raises no constitutional concerns. The chapter closing this Section presents legal challenges and possible directions for privacy protection in the example of the new Ambient Intelligence technologies.

More specifically, Christopher Suarez in Chapter 10 examines the privacy risks associated with the use of RFID in the hospital setting. He begins by presenting case studies suggesting that the application of this technology improves medical processes, decision making, and resource management. However, he points out that these efficiency gains do not come without privacy costs. In order to evaluate these costs, he draws on the literature on consumer RFID privacy to establish a set of principles guiding his overall analysis. The Chapter employs a utilitarian framework that attempts to balance the usefulness of the technology with the privacy harms posed by it. In this context, the author clarifies that endorsement of the technology in one area does not necessarily imply that it is endorsed by the public in all areas. Moreover, patients should have the ability to make choices relating to hospital RFID with the fullest information possible so that acceptance of the technology reflects true endorsement. Suarez adopts a proprietary conceptualization of privacy and builds on Schwartz’s work to identify five principles against which to evaluate RFID hospital applications: limits on transferability, explicit opt-in defaults, right of exit, right of recourse, and institutions that ensure full information provision. The Chapter then provides some background on the few laws that currently govern hospital RFID in the United States. Some federal legislation only addresses RFID hospital privacy indirectly, and while thirteen states have passed RFID legislation as of 2010, most of it does not address RFID hospital privacy matters in a comprehensive fashion.

Against this backdrop the chapter then assesses a number of RFID hospital applications. The discussion begins with asset management. The author distinguishes between asset management for general hospital assets and that for patient assets. The latter is different because patient assets must be associated with patients to be used effectively in the hospital. Suarez address two such examples, hospital blood inventory and patient pharmaceuticals, and advocates a much more rigid privacy analysis of these applications. He then turns to the question of “human tagging.” He distinguishes between implantable and external tags and highlights the more serious privacy implications associated with the former. Last, he examines RFID applications within neo-natal intensive care units, long-term care centers for the elderly, and emergency and operating rooms. In the concluding section, the author offers procedural and legal recommendations and suggests that additional pilots need to be undertaken within hospitals to assess how beneficial RFID really is.

Chapter 11 examines the implementation of RFID technology in the registration of all motor vehicles in the Philippines. It maintains that the passive use of this technology in this context does not threaten protected privacy zones in the Philippine constitution and relevant statutes. Diane Desierto first provides some background on the Land Transportation Office’s (LTO) RFID tagging system: an RFID tag attached to a motor vehicle would enable LTO personnel with RFID readers to more swiftly retrieve registration
information pertaining to the vehicle from the LTO databases, such as the motor vehicle file number; engine number; plate number; motor vehicle type; owner name; last registration date, etc. Petitioners in Bayan Muna et al. v. Mendoza et al. argued that this system constitutes an impermissible intrusion on people’s protected zone of privacy. According to them, the threat to the right to privacy of citizens exists from its potential misuse for unauthorized governmental surveillance. However, as Desierto explains, these fears are unsubstantiated: passive RFID tags have narrow operational capabilities in that by themselves they do not store any other information about the driver of the vehicle. All that is signaled from the RFID tag to an RFID reader is a “unique serial number” that enables access to what has long been publicly-available and accessible registration information in the LTO’s motor vehicle registration database. The author emphasizes the public availability of this information: even if a third party were to physically acquire an LTO personnel’s RFID reader and use it to scan RFID tags on motor vehicles, he or she would not be accessing information privileged against public disclosure.

The Chapter then evaluates the constitutionality of the application of this technology based on the jurisprudence of the Philippine Supreme Court. That Court has adopted the “reasonable expectation of privacy” test enunciated by the US Supreme Court in Katz. According to this case-law, “[t]he reasonableness of a person’s expectation of privacy depends on a two-part test: (1) whether, by his conduct, the individual has exhibited an expectation of privacy; and (2) whether this expectation is one that society recognizes as reasonable.” In the Philippines, as Desierto points out, motor vehicle owners have long been put on notice by Congress that the LTO can physically inspect vehicles to determine their registration; therefore, they bear necessarily lower privacy expectations. The reading of a passive RFID tag attached to a motor vehicle is analogous to such routine inspection. The Chapter concludes that the implementation of a passive RFID tagging system serves a public purpose in advancing governmental efficiency through expediting and facilitating access to registration information already available to the public, without granting to the LTO any power that it does not already possess.

Chapter 12 discusses legal challenges that the new Ambient Intelligence technologies (AmI) are likely to raise with respect to privacy, and seeks to offer directions for potential solutions. Shara Monteleone first provides a definition of Ambient Intelligence as “a digital environment that proactively, but sensibly, supports people in their daily lives.” Based on the use of sensors networks, wireless communications, smart devices, the central idea of AmI is to reduce the size of computers, so that they can be embedded in familiar objects, and employ the augmented computation capacity so as to provide a mixed, real-virtual experience that “should” improve the way we can benefit from our living surroundings. AmI entails privacy implications because, for example, tracking, locating, and identifying specific people in a certain environment has become essential in the new AmI systems in order to provide services according to the situations, needs and preferences of different users. The author then examines the concepts of privacy and data protection. She notes that “privacy” is still a muddled concept and that data protection legislation has introduced a more dynamic dimension of privacy that gives to data subjects the right to control the use of their personal information. The Chapter endorses Solove’s pluralistic conception of privacy, whereby what we consider as entitled to privacy protection is variable according to time, values and technologies. It subsequently offers an overview of certain international and European legal instruments according to privacy and data protection the nature of fundamental rights.

Monteleone recommends the adoption of sector-based legislation at the EU level, especially in the context of AmI technologies. She explains that their new possible deployments and their convergence with other technologies could be better managed at a specific rather than a general level. This contextual approach advocates for a system of “micro-policies,” without however sacrificing coherence. The
author makes clear that this adaptation of privacy preferences to contexts and users should not suggest a proprietary understanding of privacy viewing privacy rights as a “package” similar to other services. Furthermore, she assesses the legal-technical approach which she finds convincing, but observes that it comes with challenges of its own. Last, the Chapter touches on the tension between privacy and security and suggests that the future development and use of AmI technologies in this context will probably exacerbate this tension.

Section Five returns to the discussion of privacy risks and protection in networks. The emphasis, however, this time is not on conceptual questions but more on specific policies, their effects and the need for reforms. The examples analyzed in this Section are the protection of children’s privacy online and digital copyright enforcement.

In Chapter 13 Federica Casarosa begins by acknowledging that children might be techno-savvy but are also particularly vulnerable to privacy violations on the Internet. Increasing the safety of the online environment requires a multi-pronged approach, but the chapter focuses on one aspect of such protections: the informative privacy notices (or “privacy policies”) on websites that collect personal data. The author first compares the EU and the US approaches to children privacy. In the EU the regulatory framework (most notably the Data Protection Directive) does not directly address the problem of children privacy as it applies uniformly regardless of the age of users. On the contrary, in the US the Children's Online Privacy Protection Act provides special protection for children under the age of 13. In order to evaluate against neutral and uniform criteria the privacy policies of websites based in Europe and the US, Casarosa uses as benchmark the pertinent OECD “fair information principles”: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, accountability. She further distinguishes between websites targeting children directly, websites of a general audience where children and young people are addressed only in a limited part of the website, and social networking websites. The Chapter reaches a number of conclusions: for instance, websites tried to clarify the main elements of the privacy policy; however, in terms of clarity and readability, only in few cases could the privacy policy be considered highly understandable and none of the analyzed privacy policies were directed to children. This prompts the author to suggest improvements, namely child-targeted design and multi-layered privacy policies. A layered structure would allow for notices drafted in a simple and clear structure easy for children to navigate. Providing minors with a more easily readable, and consequently understandable privacy policy, the author concludes, could improve their capability to engage in critical analysis and reach a really “informed consent” to provide their data.

Chapter 14 analyzes the tension between digital copyright enforcement and privacy. Pedro Pina notes that in the past such a conflict would be hardly imaginable. Digitization, however, has changed in quality and in quantity the possibilities of copyright infringement. Facing massive online copyright infringements, mainly by file-sharers on peer-to-peer (P2P) systems, rightholders started developing more and more intrusive new enforcement strategies in electronic communications. In turn, digital copyright laws adopted the legal-technological approach for protecting creative expression. However, intrusive technological measures created to identify online infringers might put in risk the privacy sphere of internet users, since their navigation and identification data can be collected and treated by a copyright holder. Pina reads the EU legislation in this field to assume that collecting IP addresses is a lawful rightholder’s behavior if functionally directed to subsequent copyright enforcement, since in the context of P2P networks it will be the adequate means to present “reasonable evidence.” On the other hand, he points to the European Union’s concern over the protection of personal data and argues that IP addresses must be considered personal data. The Chapter also discusses a decision by the European Court of Justice holding that EU
law does not require Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. This approach, according to the author, indicates that a balance between copyright enforcement and personal data protection is required by EU law. Last, the chapter addresses the graduated response mechanism, according to which, online warnings are sent to the subscriber potentially committing copyright infringement, whereby he/she is advised about the illegality of his/her behavior. If the infringement continues, six months after the first warning, a new one is sent. If, even so, the unlawful activity continues, in the last step of this procedure, a court may order the suspension of the broadband accounts of file-sharers of copyrighted material online. Pina suggests that this can be an appropriate alternative only if it respects the data collecting and treatment principles, and the general principles of proportionality, necessity and adequacy. The obligation of ISPs to filter data content should require a prior court decision, and the mere collection of IP addresses should similarly need previous authorization.

Different chapters have previously alluded to the protection of privacy and personal data in the European area. Authors have invoked EU law either as a part of the applicable legal regime or as a model providing directions for reform in foreign jurisdictions. The focus of Section Six is now specifically on different aspects of privacy protection in the European space. Although EU law is generally perceived to offer high standards of protection in this area, the chapters in this Section also touch on the occasional limitations of the EU legal framework in providing effective privacy protections.

 Nóra Ní Loideain begins this inquiry in Chapter 15 by analyzing the Data Retention Directive (2006/24/EC). This Directive requires the retention of every European citizen’s communications data, including traffic data of communications and location data of the communication devices used, for up to two years for the purpose of police investigation. The Chapter first presents the background and the origins of the Directive. Its legislative development, Ní Loideain observes, demonstrates the considerable unease among legislators and non-governmental organizations surrounding the Directive. The European Parliament’s initial report to the Commission contained several proposals restricting the scope, amount of data, access to data and the period of retention as proposed by the Council, but the Council did not take into account a significant part of these proposals. The author then outlines the main provisions of the Data Retention Directive pertaining to access, the period of retention, security and oversight mechanisms, and the evaluation of the application of the Directive by the Commission. She subsequently sets out the substantive principles of European data protection legislation and explains that against this backdrop the Directive in question raises serious concerns: no systematic and reliable empirical research was carried out and used in its legislative development; the significant scope of the retention period increases the prospect of inappropriate searches by law enforcement officials and others; the data is not only accessible to “competent national authorities,” but is also subject to access by members of the private sector as this communications data must be retained, processed and made accessible to each Member State by private ISPs. Ní Loideain suggests that the Directive raises further concerns under the European Convention on Human Rights as it would fail the proportionality test. No empirical evidence has been put forward to establish the necessity for such unprecedented invasions of privacy. Moreover, the Directive entrenches the practice of blanket surveillance of the communications of all citizens and not just those under suspicion. In conclusion, the author recommends that the National Data Protection Commissioners undertake annually an empirical study that would measure the effectiveness and necessity of using such retained communications data, particularly the number of times in which this information was essential in the successful prosecution of serious crime.
Chapter 16 discusses the EU data protection regime as well as the pertinent jurisprudence of the European Court of Justice. As Maria Tzanou clarifies, the protection of personal data at the EU level is increasingly conceived of as an autonomous fundamental right, distinct from the right to respect of private and family life. The Chapter first presents the constitutional framework for the EU data protection regime, that is, the relevant Treaty provisions. It then moves on to the legislative instruments: it begins with the most important data protection initiative, the Data Protection Directive, which brings together two seemingly conflicting principles, free trade and data protection. The author discusses the background of the Directive, the history of its legislative development, its scope, principles, and definitions. With respect to the latter, she criticizes certain uncertainties still existing regarding the definition of “personal data” and “processing.” Other documents studied are the e-Privacy Directive that applies in the electronic communications sector, and Regulation 45/2001/EC that applies to the processing of personal data by EU institutions and bodies. Last, Tzanou addresses the Data Retention Directive which, she concludes, interferes disproportionately with the right to privacy.

The second part of the chapter analyzes the case law of the European Court of Justice in this area. The author notes that the ECJ has generally interpreted in a generous manner the Data Protection Directive to ensure a high level of protection of personal data within the EU legal order. As she puts it, the Court has interpreted an internal market harmonization instrument in such a manner that fosters the protection of a fundamental right within the EU. For example, it has adopted a wide interpretation of the protective scope of the Directive to cover activities regardless of their connection with the internal market as well as to apply the privacy safeguards to new technological developments, and in particular the Internet. Moreover, Tzanou refers to the jurisprudence of the Court requiring the balancing between data protection and other rights and principles, such as freedom of expression, transparency and public access to documents. The last section of the Chapter discusses the transfer of data to third countries which, pursuant to the Directive, depends on whether the third country in question effectively ensures an “adequate level of protection.” Tzanou argues that the adequacy principle ensures, in principle, a high level of protection of the right to privacy in transborder data flows. She concludes by critically assessing the PNR cases concerning the obligation of airlines operating transatlantic flights to provide “Passenger Name Records” data to the US customs authorities.

The following chapter of this Section and the book continues on the topic of cross-border transfers of personal data. Although Chapter 17 focuses on the Romanian legal regime, the presentation therein can, in large part, be generalized to cover other European jurisdictions since Romania implements the EU legal framework for data protection. Grigore-Octav Stan and Georgiana Ghitu begin by presenting the main features of the Romanian Data Protection law transposing the EU Data Protection Directive. They discuss its scope of application and the general principles for personal data processing: good-faith and lawful processing, legitimacy, proportionality, accuracy, limitation, security. They make a special mention to the stronger protections applying to the processing of sensitive data as these categories of data are considered likely to trigger special risks for the data subject.

The chapter then examines the legal requirements with respect to trans-border data flows. For this transfer to be lawful, a two-step procedure is required that consists in identifying: (i) a legal basis for carrying out a data transfer under the national law of the country of export; and (ii) a legal basis for the international transfer so as to ensure that the transferred data will enjoy “adequate protection” in the country of import. As to the first step, the authors explain that data transfer represents a form of data processing and, consequently, a lawful transfer of personal data will have to comply with all legal requirements for processing. For example, the data subject must generally be informed of and consent
to the processing. As to the second step, the authors describe that, similar to the EU Data Protection Directive, the Romanian Data Protection Law sets out the general rule that cross-border transfers of personal data are permitted only if the receiving country ensures an adequate level of protection. All the countries in the EU and the European Economic Area are deemed to offer an “adequate level of data protection.” In the case of transfers to non-EU/EEA countries, the European Commission is entitled to consider that certain countries have data protection regimes providing a presumption of adequacy for personal data exports. In the absence of such an assessment, the national data protection authority is able to determine such adequacy. The authors discuss last the case of third countries not ensuring an adequate level of data protection. In this scenario, under EU and domestic law the transfer is lawful if the data controller adduces sufficient guarantees with respect to the protection of the fundamental rights of individuals. Such guarantees must result from contractual clauses included in agreements between the data exporter and the data importer.

This section concludes with Anna Pateraki’s comparative approach on the subject of the implementation of the EU legislation concerning data protection in Chapter 18. The author provides an account of the current legislative position of data protection in several EU Member States as Germany, Great Britain and France, aiming in providing the reader with information regarding the different legal ‘culture’ in the European privacy protection.

The book in its totality had three respective aims. The first one was to engage with some of the most modern and pressing privacy and technology issues. The second one was to offer—as much as possible—an international approach on these issues, in order to combine, American and European literature in the common, globalized problem of the limits that technology is nowadays imposing upon the privacy of the individual. The third was to offer not a uniform but a pluralistic approach on the value and concept of privacy. As far as the first and second aim are concerned the book has tried to offer aspects of the privacy-technology problem, at least some of the main ones from several jurisdictions and legal traditions, knowing that they can only partly cover the rapidly evolving subject of privacy and technology. Without adopting a technophobic attitude towards the subject, the implications of the rise of technology on the protection of privacy were examined in the paradigms of cyberspace, genetic, medical privacy and abortion, surveillance in public spaces and telecommunications, tagging and identification problems from the use of ambient technology, the protection of privacy in the field of digital copyright and children’s privacy, while the current subject of data protection in the EU and in specific European legal orders were analyzed. Nevertheless, numerous more subjects concerning the use of technology in the field of penal law as a means of crime detection, prevention or even penalization arise from the difficult conciliation between privacy and technology. New methods of surveillance as the electronic tracking of asylum seekers performed in Australia, the use of Carnivore, a web-surveillance used in the USA, the globalized use of Echelon, of the Global Positioning System (GPS) as well as the unauthorized use of thermal imaging devices, as shown in cases such as Kyllo vs U.S. (533 U.S. 27, 2001) present the pressing and yet constantly evolving, vast and open nature of the clash between privacy and technology. The contributions of this book examine many of these developments, leaving aside others, trying to find the advantages and disadvantages, the dead ends and the policies that we can introduce in order to manifest the ambiguities that the rise of technology creates for the privacy, freedom and autonomy of the individual. The book also offers a taxonomy of possible threats and harms to the privacy of the individual and a taxonomy of clashing aims and interests that should be taken into account when privacy values are protected. Though it is inherently fragmented, this attempt to taxonomize these extremely complex issues is finally leading the authors in a common conclusion: any attempt to ‘exchange’ privacy in order
to serve aims such as public security, the public interest, crime prevention will ultimately result in the
declination of both. The public sphere, the public aims can not sufficiently exist without the notion and
protection of the privacy, the private sphere.

One of the most ambiguous subjects in the privacy rights theory is that concerning the concept and
value of privacy. For many theorists, privacy is a chaotic notion, extremely vast, torn between the interest
of philosophy, law, sociology, psychology and even medicine. Though, the basic aim of the book was not
to address this still open theoretical and scientific debate, the multiplicity of the contributions concerning
privacy seems to conclude with a pluralistic understanding of privacy as proposed in theory by the influ-
ential article of D. Solove’s ‘Conceptualizing Privacy’, published in 2002 in the California Law Review.
Under this pluralistic rubric, privacy can not be identified as a sole concept but as a network of concepts
and understandings that take into account the relative social and legal transformations. This pluralistic
account of privacy is presented in the book that follows, via the different approaches that the authors
are adopting concerning privacy. Thus, many of the contributions adopt the traditional understandings
of privacy, as (a) ‘right to be left alone’ or as loneliness and isolation, as (b) limited access to the self,
as (c) data-privacy or control over ones personal information, as (d) intimacy and (e) personhood. At
the same time, many other aspects of privacy are presented, including its relation with autonomy (most
prominent in American theory and jurisprudence), its connection with personality, dignity and identity
(which characterizes the European approach to privacy), its shared and ‘caring’ character in the intimate
private sphere relations, such as the family, among others.

Nonetheless, the most important aim of the book was to present and apprehend the value of privacy
in the new technological era, in order to evaluate the reason why its protection must be taken seriously
in any legislative or public policy utilizing technology, or aiming in protecting public safety or public
security. Privacy protects our identity, our inner self, and the relationships that we deem as important or
crucial or as defining of how we have become and who we are now. It enables us to express ourselves
freely, to autonomously form our choices, and to independently shape our own mode and rhythm of
living. Privacy is the ‘home’ in which we create, in which we can be our true selves, in which we can
relax, even hide from the obligations and duties of the public sphere. Privacy lies in the centre of our self
and of the way we are presented and communicate with our intimates, the society, and the world. Each
contribution of this book has aimed in examining this very value of privacy from a different aspect, a
different point of view. It is after all the value of privacy that makes us remember that technology is not
a value it self. Instead it becomes worthy only because of the aims and values that it serves.

Keeping this thought in mind, we hope that the following pages with their broad coverage of a di-
verse range of legal topics, various technologies and different legal orders will provide the reader with
some directions to address the complex question of the interface between privacy and technology in
today’s world.

Christina M. Akrivopoulou & Athanasios-Efstratios Psygkas
Thessaloniki and New Haven, July of 2010
REFERENCES


