The handle http://hdl.handle.net/1887/20288 holds various files of this Leiden University dissertation.

**Author:** Klitou, Demetrias  
**Title:** Privacy-invading technologies: safeguarding privacy, liberty & security in the 21st century  
**Date:** 2012-12-14
1 Introduction

1.1 PROBLEM STATEMENT

Since the beginning of the 21st Century, as a result of the growing development and deployment of technology, the following new privacy issues or threats have arisen in the US and the UK/EU:

- A digital data trail is generated by each and every person and automatically stored.
- Law enforcement agencies are routinely using mobile phones as a tool to either track people or record their geographic location in real-time. Mobile phones are also capable of being used to record conversations (even when turned off).³
- Vehicles are being tracked via ALPR systems and/or via GPS tracking devices without a warrant.
- Banks have begun testing the use of fingerprint scanners to authenticate identity, while supermarkets are also testing biometric payment systems.
- RFID microchips are being embedded within a variety of consumer goods, and RFID microchips have been approved for human implantation.
- Plans are in place to ensure that each and every person in the US will have an electronic health record.
- Advanced face recognition systems are being integrated into CCTV cameras.
- High-powered microphones and loudspeakers are also being attached to CCTV cameras, as the deployment of CCTV surveillance systems rapidly increases and their surveillance capabilities expand.
- DNA databases are rapidly growing and DNA analysis can reveal limitless amounts of information about a person.
- Children are increasingly being digitally fingerprinted and tracked at school.

- Corporations are not only retaining vast amounts of data regarding their customers, but are also providing governments with access to their databases.
- Companies are engaged in the vast data mining of online activities and information, and online social media networking websites can track Internet surfing habits.
- ‘Fusion Centers’ and data centers capable of enabling “total information awareness” have been established in the US, as governments are expanding their surveillance and intelligence gathering authority and activities.
- Stories of Western governments conducting surveillance of private electronic communications (emails, etc.) are now commonplace.
- Body scanners capable of seeing beneath clothes are being deployed at airports around the world.
- Devices capable of enabling the user to see through walls are being developed and deployed.
- UAVs, with built-in advanced cameras, are being deployed for domestic surveillance, and law enforcement agencies are increasingly calling for their widespread use.
- Neurotechnologies may one day be capable of being used for reading our thoughts.
- Devices are being developed that are capable of recording and storing video of an entire human life.

While the above list of privacy threats/issues is certainly far from exhaustive, they involve the unprecedented development/deployment of advanced technologies, systems and infrastructures that are highly capable of being used to violate an individual’s right to privacy and pose the newest, and arguably one of the most serious, threats to liberty in modern Western society. Governments, businesses and consumers/citizens increasingly seek to take advantage of the apparent public security/safety, health, social, environmental, commercial and other societal benefits these technologies offer. But, at the same time, governments and businesses (i.e. those who can control the development/deployment of technology) must also sufficiently aim to minimize the privacy threats and societal implications of the widespread advancement, deployment and use of these technologies.
1.2 CENTRAL THESIS

Backed by case studies and overall analysis, the thesis of this dissertation is centered on the general underlying problem that technology is evolving faster than the laws that aim to regulate their use and, as a consequence; the laws are behind the advancement of technology. With the rapid advancement of technology or the inertia of technological development, the current laws and regulation strategies/approaches are increasingly becoming outdated and there is potentially no end in sight. One reason is that lawmaking is normally a gradual process and is primarily reactive, rather than proactive. In addition, the focus is all too often on the implications of the use of technologies, as opposed to the implications of the development of the technologies in the first place.

Privacy/data protection laws are essentially a perfect case in point. The current legal framework, pertaining to privacy/data protection in the US and the UK/EU, focuses predominantly on data controllers/processors, service providers and operators, and traditional policy or legal-based solutions, for the sake of privacy, are mainly focused on the users of privacy-invading technologies, as opposed to the developers/manufacturers. Hence, the Privacy Act 1974 and the Directive 95/46/EC do not apply to the developers/manufacturers of privacy-invading technologies (PITs) or ICTs. This approach may diminish or deter the unlawful or illegitimate use of these technologies, but it may also fail to address the privacy-intrusiveness of the technologies concerned at the design stage. Often, current attempts to regulate the privacy-intrusiveness of the technologies concerned are based on limited technical solutions “bolted on” after a public outcry or significant privacy breach. But, it seems that without robust and comprehensive technical solutions for implementing the principles of privacy, the relevant privacy/data protection laws are increasingly ineffectual.

As this dissertation aims to demonstrate, the law should move away from focusing primarily on data controllers and users/operators of privacy-invading technologies/ICTs and should instead impose technical/design obligations, known as “privacy by design” (PBD) requirements, on the manufacturers/developers. The concept of PBD and the PBD requirements should also be technologically neutral (as much as possible). Demonstrated through case studies, the premise is that privacy laws, directly applied to the manufactur-
Introduction

ers/developers and the design/development of PITs, can more effectively protect privacy against the threats posed by existing technologies and also have, at the same time, a better chance of staying apace with the ever-increasing technological threats to privacy posed by future and emerging technologies. Privacy/data protection laws only applied to data controllers and users/operators of privacy-invading technologies/ICTs are constantly and increasingly falling behind new technological developments.

Although there are standards and legal requirements with regards to data security and audit mechanisms thereof, the other principles of privacy are generally left out. The technical emphasis, at present, found both in law and industry standards, is all too often focused on data security alone. While existing laws may ultimately have an indirect effect on the manufacturers (e.g. data controllers can put pressure on ICT manufacturers to develop privacy-friendly technologies), this has evidently proved insufficient.

This dissertation attempts to address both the general underlying problem and specific threats to privacy and civil liberties in the US and UK, posed by the latest and evermore evolving privacy-intrusive technologies. In doing so, the dissertation also offers some potential solutions, both legal/policy and technologically/architecturally-orientated, to address the privacy threats and current legal dilemmas and to provide some answers to the key research questions (see: section 1.3).

Essentially, the dissertation shows how and why laws that focus on the design/development of PITs may better ensure the protection of privacy and better ensure that the legal framework remains more up-to-date than laws only applied to data controllers/users. The premise is supported and demonstrated through case studies (see: PART II, Chapters 5, 6 and 7). Furthermore, the dissertation overall attempts to show how laws/ regulations that mandate the implementation of PBD could potentially serve as a viable approach for collectively safeguarding privacy, liberty and security in the 21st Century (see: PART III, Chapters 9 and 10, for further information). However, while the dissertation clearly advocates for the implementation of PBD, it does not ignore the fact that the PBD approach has its own shortfalls and is not a panacea for all issues related to privacy intrusion (see: sections 9.11, 9.12 and 10.19).

It is important to note that the premise of the dissertation was only developed after the legal analysis and assessment of the case studies was completed; during which it was consistently determined or revealed that technical/design solutions (i.e. PBD solutions) could play a more important role than traditional legal solutions for regulating PITs. This determination was not planned or deliberate at all, which explains why the concept of PBD is not clearly or specifically integrated or discussed in most of the chapters.

The dissertation focuses on the following four privacy-invading technologies (PITs) as case studies:
- Body scanners;
- Public space CCTV microphones;
- Public space CCTV loudspeakers; and
- Human-implantable microchips (RFID implants/GPS implants)

Furthermore, as demonstrated through the case studies, the dissertation also argues that both privacy and other civil liberties, on the one hand, and (public/national) security, on the other, can be safeguarded.

1.3 RATIONALE BEHIND THE SELECTION OF THE CASE STUDIES

Some technologies may be regarded as the ‘black swans’ of PITs, i.e. those technologies that immediately stand out due to their disruptive or controversial and highly-intrusive capabilities and due to their immense societal impacts.\(^5\) This dissertation will focus especially on some of the foremost threats to privacy posed by the following PITs, which are considered to be ‘black swans’: Human-implantable microchips (RFID/GPS implants); Body scanners; and public space CCTV microphones and CCTV loudspeakers.

Without adequate safeguards, these technologies, and the associated acts of widespread human tracking, full body scanning, audio recording and disturbing people’s ‘right to be left alone’ out in public, could arguably pose some of the most serious technological threats to privacy and liberty in the early 21st Century. Therefore, these technologies require further scrutiny and deserve attention from lawmakers/policy makers in the very near future.

These specific PITs were chosen as the case studies for this dissertation, as a result of the controversy surrounding their increasing deployment and use, their novelty, their highly-intrusive capabilities, the various apparent legal challenges to regulate and/or curtail the associated novel privacy-intrusive capabilities, and the lack of substantial study regarding their escalating development, deployment and use.

The current focus on the privacy concerns of social networking sites, and other online/digital services, has generally ignored the fact that body scanners have rendered clothes obsolete, RFID potentially enables every object or person to be identified and tracked, the integration of microphones with CCTV cameras enables conversations out

---

\(^5\) Nassim Nicholas Taleb equally used the term “black swan” to refer to highly-improbable events that are unpredictable and have an immense impact on society, but their occurrence is believed to be more predictable and less random than they really are. see Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly-Improbable* (Random House, 2007)
in public to be recorded, and CCTV loudspeakers provide CCTV camera operators the immense ability to disturb or scold individuals from afar. The radical privacy-intrusive capabilities of these selected PITs and their enormous potential for abuse or their ‘function creep’ propensity are resulting in unprecedented intrusions into both our private and public space, threatening not just the right to privacy, but other civil rights and our freedom and personal dignity overall.

It may be argued that body scanners, public space CCTV microphones and CCTV loudspeakers and RFID implants were foreseen. For example, the concept of “x-ray specs” or “x-ray glasses”, allowing the wearer to see through objects or clothes, was envisioned decades ago. In addition, George Orwell, in his book *Nineteen Eighty-Four*, conceptualized “telecreens” (two-way screens complete with microphones and loudspeakers), which surrounded the masses, in order to monitor and control their behavior in public spaces. These PITs, therefore, could also be deemed ‘black swans’, if looked at from Taleb’s viewpoint, since their deployment now seems quite predictable, but in actual fact their development and deployment depended on various unpredictable events occurring. For example, the widespread deployment of body scanners in the US depended on the occurrence of 9/11 and the “Christmas Day attack”, which were essentially both unpredictable, regardless of the different apparently “obvious” explanations developed subsequently.

In addition, the selected PITs offer potentially significant (public/national) security benefits, which cannot be overlooked. Indeed, body scanners and public space CCTV microphones and CCTV loudspeakers are primarily used by law enforcement agencies. Therefore, by addressing or minimizing the threats to privacy and liberty posed by these PITs, we are facilitating their deployment and public acceptance and, as a result, also potentially helping to safeguard (public/national) security.

PITs mainly concern either the public sphere or the private sphere. The choice of PITs also allows the dissertation to cover both spheres (see Chapter 4 for further explanation). With regards to the private sphere, the changing level of privacy we enjoy over our bodies is explained, with the deployment and use of body scanners as the case study. With regards to the public sphere, the changing nature of the public space and level of privacy we enjoy in public is explained, with the deployment and use of public space CCTV microphones and CCTV loudspeakers in the UK as the case studies. Human-implantable microchips (RFID/GPS implants) concern both the private and public sphere, since HIMs and the corresponding infrastructure impact the nature of the

---

6 Ibid.
public space and of the human body, and radically change the level of privacy enjoyed in both spheres.

The US and the UK were chosen as the country case studies or legal jurisdictions, on the grounds of actual technological threats and since it is where the chosen PITs are largely being deployed. Both the US and UK needed to be covered, since body scanners and HIMs are predominantly being deployed in the US, while public CCTV microphones and CCTV loudspeakers are predominantly being deployed in the UK. The UK is leading the way in the deployment of CCTV public surveillance systems. For example, London’s so-called “ring of steel” has served as a model for New York City’s CCTV public surveillance system (Cannataci, 2010).

Moreover, the US and the UK were selected as the country case studies, since both countries are also leading the way in the establishment of a ‘surveillance society’. Privacy International, a watchdog on surveillance and privacy, for their 2007 International Privacy Ranking, gave the UK and the US a final score of 1.4 and 1.5 respectively (out of a score range of 1-5, with 1 indicating a surveillance society and 5 indicating a society where privacy is ideally upheld). The final scores of the US and UK were practically equal to the final score of China with 1.3. The UK, in particular, had the lowest score in the EU and, as the UK Government moves to monitor all online activities, this score should be even lower. The UK already has millions of public space CCTV cameras deployed and operating, and the UK’s former Information Commissioner, Richard Thomas, himself is well-known for often declaring that the UK is “sleepwalking into a surveillance society”. As the leader in the overall development and deployment of PITs, the US is certainly not far behind.

The focus on both the US and the UK also allows for a broader audience. Since the UK is an EU Member State, there is also an opportunity to briefly show some of the differences between the US sectoral approach and the current EU comprehensive approach to privacy protection and to take into account legal precedent of the European Court of Human Rights (ECtHR), where necessary.

---


8 see “Internet activity ‘to be monitored’ under new laws” (The Telegraph, 1 April 2012), available at: http://www.telegraph.co.uk/technology/news/9179087/Internet-activity-to-be-monitored-under-new-laws.html
1.4 KEY RESEARCH/EVALUATION QUESTIONS

The following are the general underlying research/evaluation questions the dissertation aims to broadly address:

- What changes to society are brought about by the increasing advancement and deployment of the most intrusive PITs?
- How will the latest PITs impact the right to privacy and other civil liberties?
- How can the right to privacy and other civil liberties be ensured?
- What are the main limitations of the right to privacy and/or data protection laws?
- Should new laws be adopted or can existing laws be applied to the new challenges and threats posed by the latest PITs?
- Are the existing fundamental principles of privacy still relevant? If so, how can we uphold the principles of privacy, in light of the threats and challenges posed by the latest PITs?
- How can both security and the right to privacy and other civil liberties be ensured/safeguarded (in practice and in theory) for the 21st Century?

The following are some of the specific questions addressed:

*Body scanners*

- In what way is the use of body scanners legal and illegal?
- How should the use of body scanners be regulated to ensure the right to privacy and freedom from unreasonable search and seizure?
- How can both privacy and the effectiveness of body scanners in airport security screening be maintained?
- Are there viable alternatives?

*Public space CCTV microphones and loudspeakers*

- How does the use of public space CCTV microphones and loudspeakers involve the right to privacy and privacy laws?
- How can the deployment and use of CCTV microphones and loudspeakers be regulated?
Human-implantable microchips (RFID/GPS implants)

- In what way human-implantable microchips (HIMs) alter the nature of the human body?
- To what extent, are RFID/GPS implants a threat to privacy, liberty and human dignity?
- Should RFID/GPS implants be banned? If not, how should RFID/GPS implants then be regulated? What amendments and additions in the legal framework must occur in order to adequately regulate RFID/GPS implants and defend the right to privacy/data protection and other civil liberties?
- When is the tracking of individuals legitimate and illegitimate? When is the use of RFID/GPS implants to identify and track people legitimate and illegitimate?
- Can the government potentially force prisoners or criminals to be implanted? Does the government have the right to order citizens to be implanted for identification purposes? Do employers have the right to dismiss an employee who has refused to be implanted for access control purposes? Should parents be allowed to impose RFID/GPS implants on their minor children?
- When is location information (generated by HIMs) personal information? What is the expectation of privacy for location information?
- Should the criteria of a “reasonable expectation of privacy” and determination of a privacy intrusion be revised?
- How are the private space and public space and the physical world and virtual world potentially merging? What approach can accommodate for this potential merger?

1.5 RESEARCH OBJECTIVES

The overall research goals of the dissertation are:

- To evaluate/assess the legal framework for the protection of privacy in the US and UK (EU) in light of the latest PITs;
- To identify and recommend suitable enhancements, amendments and additions to the US and UK (EU) legal frameworks for the protection of privacy, taking into account the development and deployment of the latest PITs;
- To define an approach for striking a balance between privacy and other civil liberties, on the one hand, and security, on the other.
1.6 RESEARCH METHODOLOGY AND APPROACH

The dissertation somewhat attempts to take a multi-disciplinary approach, with the aim of bringing together several different fields, including law, human rights, international relations, social science, political science and computer science. But, the dissertation generally avoids the social and moral criticism of the rapid development and deployment of PITs. Without arguing against the deployment of PITs, the dissertation instead aims to focus primarily on addressing the legal issues at hand and on proposing practical solutions for ensuring that privacy/liberty is upheld.

For each PIT this dissertation specifically addresses as case studies, their privacy-intrusive capabilities, based on ordinary desk research, are explained and described. Then, the relevant statutory laws, regulations and case law on privacy protection, within either the US or the UK, of special relevance to each of these PITs, are identified and outlined. The case studies for this dissertation specifically include: human implantable microchips (GPS/RFID implants); body scanners; and public space CCTV camera microphones and loudspeakers.

In order to achieve the research objectives and address the key research questions, the adequacy of the legal frameworks of the US and the UK is assessed, in light of the identified intrusive capabilities of the four latest PITs, specifically addressed as case studies. The assessment of the adequacy, and ensuing determination of the deficiencies and dilemmas of the US and UK legal frameworks, is based on the criteria outlined and defined in Chapter 3. The criteria are based on the fundamental principles of privacy and other legal principles/requirements. The policy recommendations on enhancing the legal frameworks, in light of the privacy-intrusive capabilities of each PIT, are subsequently formulated, equally based on the fundamental principles of privacy and the identified legal deficiencies and dilemmas. For body scanners and human-implantable microchips, the US legal framework is evaluated. For CCTV microphones and CCTV loudspeakers, the UK/EU legal framework is evaluated.

The same criteria are used for each PIT for assessing the legal frameworks, in terms of privacy protection, and for determining the required solutions, amendments and additions to enhance the legal frameworks. However, the layout for the separate chapters covering each PIT is not identical, given that the overall privacy implications, intrusive capabilities, circumstances and potential solutions/recommendations that need to be considered, concerning the use and deployment of each PIT, are different.
The problems, root causes, objectives, recommendations and countermeasures addressed by this dissertation are mapped out and summarized in an A3 Report9 (see: Annex I). It is important to note that the A3 Report was developed only after the overall research findings and conclusions were established. Moreover, the overall conclusions and overall policy recommendations of the dissertation (see: Chapter 10) are based on the specific analysis and conclusions/results of the case studies.

The dissertation attempts to take a balanced approach, in order to avoid any extreme or one-sided points of view. Moreover, in order to adopt a more balanced and scientific approach, the different points of view of a variety of stakeholders are thus taken into consideration. While the (potential) threats to privacy and other civil liberties posed by the latest PITs are emphasized, the (potential) societal and security benefits of these PITs are also pointed out.

The research formally began September 2007. Timing is critical for this dissertation, as the world, in terms of technological, policy, legal and political developments, is constantly evolving. The current state of the legal framework in the US and UK, the current state of art of the technologies addressed, and the current situation and circumstances surrounding the deployment and use of these technologies is outlined and evaluated based on the current state of affairs up until January 2010, for the most part. However, while the cut-off date is January 2010, there are some exceptions, where necessary or helpful. Indeed, since early 2010, there have been a number of legal/policy developments in the US that are relevant for the dissertation and cannot be ignored. For example, concerning GPS tracking, the US Supreme Court granted a writ of certiorari in the case US v. Jones and then later issued a ruling on the legality of the installation and use a GPS tracking device without a warrant. In addition, the EC issued an official draft of their proposed EU General Data Protection Regulation.10 Also, the FTC published the acclaimed December 2010 Staff Report, “Protecting Consumer Privacy in an

---

9 An A3 Report, named after the paper size standard on which it is meant to fit on, is an effective method of communicating a chain of reasoning and mapping out thoughts for solving problems. A3 Reports have been extensively used by Toyota Motor Corp. to understand and communicate the root cause(s) of a problem and its solutions. A3 Reports are composed of a sequence of text boxes, which, normally in the following order: (1) identify and explain the problem(s) or issue(s); (2) breakdown the current conditions and reasons (cause and effect) for the problem or issue in order to get to its root cause by asking 5 or more ‘Whys’; (3) determine the countermeasures to solve the problem; (4) establish an action plan; (5) identify the desired outcome; (6) implement the plan and follow up. The “5 Whys” technique was developed by Sakichi Toyoda and later adopted by Toyota Motor Corp.

10 see Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft.
Era of Rapid Change”, which emphasizes the role of privacy by design. Some of these more recent developments will be discussed, albeit in a limited way. Still, the dissertation generally does not incorporate additional developments after January 2010, unless where and when deemed required.

1.7 MAIN SOURCES OF INFORMATION

The main sources of information for this dissertation include at least: relevant books and published/academic papers; statutory laws, regulations, and case law; corporate privacy policies and self-regulations; commissioned privacy reports; policy papers; company websites; press releases; current events; news articles; expert views/judgment; stakeholder perspectives; surveys; public consultations; workshop/working group discussions; and conference papers.

1.8 ADDED VALUE

The research predominantly serves to determine if the legal framework for the protection of privacy/personal data in the US and UK is still effective and adequate in light of the deployment of the latest PITs. Diverging from traditional legal dogma pertaining to privacy/data protection in the US and UK, the deficiencies and dilemmas of the respective legal frameworks, particularly concerning the four specific PITs addressed (body scanners, CCTV loudspeakers, CCTV microphones and RFID/GPS implants) are identified. From there, the research proposes recommendations, which include a mixture of new laws and policies, amendments to existing laws, legal definitions and interpretations, privacy safeguards and technological solutions, in order to address the current legal issues and minimize the threats to privacy posed by these latest PITs. Overall, regardless of the PIT in question, the research aims to identify what is required in order to balance the perceived security gains of PITs with the right to privacy and other civil liberties these technologies threaten.

It is further important to note, however, that the recommended legal methods, solutions, definitions and safeguards are written, for the most part, in the form of policy-orientated proposals/recommendations, which are meant to be specific, practical and actionable. These proposals should arguably be considered, in order to enhance the

---

11 As a follow-up to the preliminary FTC Staff Report, the FTC Final Report, “Protecting Consumer Privacy in an Era of Rapid Change”, was published in March 2012, available at: http://ftc.gov/os/2012/03/120326privacyreport.pdf.
legal framework. However, while these recommendations should be considered for amending existing legislation or drafting new laws, for example, they are not written in a legislative text format, nor are equally comprehensive or technical. Moreover, while this dissertation explores the relevant legal questions and attempts to address these questions, the answers are not all complete, as some of the critical legal questions still need to be left to the courts and lawmakers to decide upon.

1.9 ISSUES AND AREAS NOT SUBSTANTIALLY ADDRESSED

Due to the limited scope of the research, this dissertation specifically does not attempt to formulate comprehensive, specific and widely agreed upon definitions of privacy and liberty. The research neither aims to substantially compare the American and European legal approaches to privacy protection for each case study or analyze the different relationships between the legislative and judicial branches of government. Besides, CCTV microphones and loudspeakers are primarily being deployed and used in the UK, while body scanners and RFID implants are primarily available in the US. In addition, the dissertation does not intend to resolve the long-standing legal debate on technological neutrality or to substantially add to the broad discussion on the advantages and disadvantages of technological neutrality. Finally, the dissertation does not include substantial discussion on the overall social developments/implications surrounding the ever-increasing deployment of PITs.

1.10 STRUCTURE OF THE DISSERTATION AND OVERVIEW BY CHAPTER

The dissertation is divided into four Parts:

- In PART I, Chapter 2 briefly explains what is meant by privacy, liberty and security, and how they are interrelated. Chapter 3 delineates the assessment criteria this dissertation applies to assess the adequacy of a legal framework in terms of protecting privacy.

- In PART II, Chapter 4 explains what is meant by privacy-invading technologies/privacy-intrusive technologies (PITs) and how PITs are altering the level of privacy we should expect in the private and public sphere, and provides an overview of technologies that may pose a significant threat to privacy/liberty. Beginning with the first case study of dissertation study, Chapter 5, addresses the implications of
the deployment and use of body scanners. For the second and third case studies, Chapter 6 addresses the implications of the deployment and use of CCTV microphones and CCTV loudspeakers. For the fourth and final case study, Chapter 7 addresses the implications of the deployment and use of human-implantable microchips (RFID/GPS implants). Altogether, PART II explains how body scanners should be considered as a strip search by other means, how public space CCTV microphones and CCTV loudspeakers can act as the ears and mouth of ‘Big Brother’, and how HIMs could seriously threaten privacy and alter the way we perceive our bodies as transmitters of information in a location-aware world. Chapter 8 sums up some of the conclusions derived from Part II.

- In PART III, Chapter 9 provides an overview of what is meant by “privacy by design” and an overview of the issues surrounding the concept.

- In Part IV, Chapter 10 concludes with the dissertation’s overall research findings, conclusions and policy recommendations, based on the results and analysis of the case studies, and a concise overview of some of the answers to the general research/evaluation questions.

In the Annexes, Annex I contains an A3 Report, mapping out and summarizing the central thesis of the dissertation. Annex II contains a summary table with a short overview of the intrusive capabilities of the specific PITs addressed and the corresponding most relevant laws and self-regulations, legal deficiencies, and proposed key recommended legal and technological solutions.

---