PReparing Industry to Privacy-by-design by supporting its Application in REsearch

Deliverable D4.1
Educational Requirements to Foster a Risk Management Culture

Project:	PRIPARE
Project Number:	ICT-610613
Deliverable:	D4.1
Title:	Educational Requirements to Foster Risk Management Culture
Version:	v3.0
Date:	29/3/2014
Confidentiality:	Public
Author:	Claudia Roda (AUP) Brian Kennedy (AUP) Susan Perry (AUP) José M. del Álamo (UPM) Pagona Tsormpatzoudi (KUL) Fanny Coudert (KUL) Hisain Elshaafi (TSSG) Frank Kargl (UULM) Henning Kopp (UULM)

Funded by the European Union's eventh Framework Programme

Table of Contents

Document History

Version	Status	Date
v0. 1	Overall structure	11.2013
v0. 2	Definition of chapter contents	11.2013
v0. 3	Added content to section 3.2	12.2013
v0.4	Added tentative work assignment to partners	13.1.2014
v0.5	Added examples of materials section4	15.1.2014
v0.6	Added content to section 3.2.1-3.2.5 and moved the courses into an appendix.	27.1.2014
v0.7	Added all partners' contributions to sections 1, 2 and 3	30.1.2014
v0.8	Added section 3.1	15.2.2014
v0.9	Incorporated Frank Kargl's comments and edits	12.3.2014
v0.10	Expanded content in Appendix 1	13.3.2014
v0.11	Added partner's content to section 4.2 and 4.4	24.3.2014
V0.12	Added themes and table to section 4	27.3.2014
V0.13	Added UULM contribution to table, general review for consistency between table and section 4. Executive summary. General review.	28-29.3.2014
V0.14	Consortium review and authorization	3.4.2014

Approval		
	Name	**Date**
Prepared	Claudia Roda	31/3/2014
Reviewed	All Project Partners	31/3/2014
Authorised	Antonio Kung	31/3/2014

Circulation	
Recipient	**Date of submission**
Project partners	31/3/2014
European Commission	day/month/year

Acronyms Table

Acronym Table	
Acronym	**Definition**
29WP	Article 29 Working Party
AFCO	Constitutional Affairs' Committee
Belspo	Belgian Science Policy Office
C2C	Car to Car
C2I	Car and Infrastructure
CEPS	Centre for European Policy Studies
CIPM	Certified Information Privacy Manager
CIPP/IT	Certified Information Privacy Professional/Information Technology
CNECT	Communications Networks, Content and Technology
CS	Computer Science
DG	Directorates-General
DPA	Data Protection Authorities
DPO	Data Protection Officer
EDPS	European Data Protection Supervisor
EDRi	European Digital Rights
EMPLO	Employment, Social Affairs & Inclusion
EU	European Union
FRA	Fundamental Rights Agency
FTC	Federal Trade Commission
GRC	Governance, risk management, and compliance
HTTP	Hypertext Transfer Protocol
IAM	Identity and Access Management
IAPP	International Association of Privacy Professionals
ICT	Information Communication Technology
IT	Information Technology

JHA	Justice and Home Affairs
JRC	Joint Research Centre
MARKT	Internal Market and Services
NGO	Non-Governmental Organization
OECD	Organisation for Economic Co-operation and Development
PbD	Privacy-by-Design
PET	Privacy-Enhancing Technology
PIA	Privacy Impact Assessment
PRIPARE	Preparing Industry to Privacy-by-design by supporting its Application in Research
REST	Representational State Transfer
RFID	Radio Frequency Identifier
RTD	Research and Technological Development
SbD	Security-by-Design
SOAP	Simple Object Access Protocol
TTE	Transport, Telecommunications, and Energy Council
UN	United Nations
WSDL	Web Services Description Language

Executive Summary

This deliverable presents the analysis undertaken by the PRIPARE consortium to define the informational and educational needs of digital privacy stakeholders. In particular we concentrate on the general public, engineering and legal practitioners, policy makers, and governmental and non-governmental bodies acting for human rights protection, as well university students in both technical and non-technical disciplines.

As a first step we have identified several sub-groups of stakeholders within the large categories mentioned above and, for each one of these sub-groups, we have identified their informational/educational needs and defined the learning outcomes that the educational material produced within the project should trigger. The general public was analysed on the basis of their level of vulnerability. Practitioners were considered in terms of their professional role, either managerial or development. The study of Students needs was based on the type of their degree (technical versus non technical), the level of study (graduate, undergraduate) and career goals. With respect to policy and legal stakeholders we have identified policy makers and governmental body acting at different geographical levels (national, European, international) as well as non-governmental bodies including NGOs, think-tanks and civil society organisations, and legal professionals.

Once stakeholders and their educational/informational needs were identified we explored the material already available in order to address their needs. A large number of online resources and publications were collected and analysed with respect to their ability to address Privacy by Design issues and our stakeholders needs in particular. We also created an inventory of existing university courses covering privacy issues in extensive / in-depth manner; we examined the material used by these courses and the type of students addressed. The most relevant reference material for policy makers and governmental and non-governmental bodies was analysed both for EU policy and non-EU policy.

On the basis of this research we identified the themes that our material should prioritise for each one of the stakeholders in order to address their educational/informational needs. These themes were classified in either *general knowledge* or *specific knowledge*. Learning material was organised in *modules* addressing one theme or part of one theme. In certain cases a module serves as a pointer to existing material while, in others, the module consists in a newly created unit, e.g. a collection of slides, an inforgraphics, a brochures, a video, etc. We expect that *general knowledge* modules created for one stakeholder may be reused for building a knowledge sequence for other stakeholders, whereas *specific knowledge* modules may only be useful for a specific set of stakeholders.

The last section of this deliverable (section 4) describes in details all the modules we aim to create during the project.

1 Introduction

WP4 "Educational Requirements to Foster a Risk Management Culture" addresses the salient need for privacy protection education for a range of stakeholders, including all sectors of the General Public, as well as Practitioners, Policy makers, and governmental and non-governmental bodies acting for human rights protection, and Students in related disciplines. The educational and reference material provided by WP4 participants will cover the relevant socio-ethical, legal and technical issues that privacy-by-design raise for these stakeholders across society.

The General Public is a heterogeneous group made up of users of digital technology who may or may not be aware that privacy protection is an issue when they turn on their tablets or Smartphone. The General Public also includes certain non-users of digital technology, such as some elderly, whose personal information is embedded in information technology systems, often without their knowledge. In order to provide educational material that speaks to this highly varied group, we will first identify subsets of the General Public (e.g. children, youth, the elderly), before targeting salient ethical issues raised by privacy violations, the legal ramifications of these violations, and how these violations may occur, may be prevented, or remedied. Educational materials and references for these subsets should be clear, easy to access and function as stand-alone pieces or as a series of materials that interact with one another.

Practitioners are those industry specialists whose work may involve them in one or more phases of the lifecycle of an information technology system or piece of software. Whether IT designers or IT users, whether managers or developers, these specialists require educational materials that explain the legal and policy framework on privacy, as well as the risks and benefits inherent in a privacy-by-design approach. System designers and implementers will also require an in-depth introduction to the technical foundations of privacy-by-design (PbD), from cryptography, over protocols, privacy-preserving data processing, to privacy-friendly human-machine interaction, so that they are familiar with the "privacy toolbox" available to be deployed during a PbD engineering project. Learning materials and references for practitioners will provide a privacy-by-design methodology that enables individuals and teams to incorporate PbD at the outset of IT projects.

Students are tomorrow's designers, regulators and users of digital technology and their professional success will require a sophisticated understanding of the challenges inherent in PbD. Students in the fields of computer science and information technology should have a deep knowledge of the technologies enabling PbD as listed above as well as a robust understanding of the legal obligations on privacy while being familiar with the EU regulatory framework on privacy protection. Students in the fields of law and public policy should be digitally literate, with a solid understanding of how IT systems function and the challenges faced by software and IT systems designers in delivering PbD. Learning materials and references for students will be aimed at both undergraduates and graduates, and require critical thinking on the trade-offs inherent in PbD for digital technology.

Policymakers, as well as governmental and non-governmental bodies specializing in human rights protection cover a wide-range of regulatory issues relating to digital technology. The educational materials and references should aim at encouraging the creation of a normative framework of privacy by default in all regulatory matters. These materials should also enable the design of clear-cut operational standards that distinguish between risk management for certain populations (adult IT users) and strict protection for others (children, for example). In

all cases, the materials should promote the European Human Rights Framework as the baseline for regulatory behaviour by government and watchdog agencies with respect to privacy by design. Furthermore, all target groups will benefit from at least a high-level awareness of the technical progress in Privacy Enhancing Technologies from recent years as this will create awareness about what is possible and that there are very often no technical excuses for designing privacy-unfriendly systems.

2 Identification of stakeholders and their needs (learning goals)

2.1 General Public

The large category of the General Public is both the most difficult to define and the most vulnerable to online privacy issues. For the development of educational materials on robust privacy rights and protection for digital technology users, we have used a needs assessment method to create categories ranging from the most to the least vulnerable groups of citizens. The most vulnerable users are children and those for whom a privacy violation could lead to physical or psychological threat (victims of domestic violence, for example). Least vulnerable citizens are those who have little interaction with digital technology (e.g., the elderly and the digitally reluctant), but whose private information is nonetheless stored online by, for example, banks, health providers, or surveillance cameras. The vast majority of the General Public is somewhere in the middle. According to a recent Pew Internet Study, "Anonymity, Privacy, and Security Online", 86% of Internet users "have taken steps online to remove or mask their digital footprints" and "68% say current privacy protection laws are not good enough"[1]. For the purposes of this project, we will focus our efforts on the privacy needs and expectations of these three groups.

2.1.1 General Public Needs

1. Vulnerable populations.

- children and vulnerable adults require educational material that clearly explains their rights, potential threats to their privacy, how to react to specific contents and situations (e.g. usage agreements, privacy policies, etc.), and where to go for immediate help should their rights be violated.

2. Less vulnerable populations.

- the handicapped and the elderly are those who stand to benefit the most from smart houses and apartments that allow for both the desired level of autonomy and a constant surveillance in case of an accident.
- as with the digitally reluctant, data generated by these citizens should be robustly protected, with appropriate protection technology and regulation that allows each individual to select the appropriate level of privacy protection for their data and/or online activities. Educational material should provide a clear indication of rights and a list of appropriate counsel to assist in selecting privacy protection levels and raise the awareness about availability of privacy-friendly alternatives.

3. General users.

- given that surveys indicate an exceptionally high level of public distrust with respect to privacy protection, educational material should provide a clear understanding of rights, a balanced assessment of the trade-offs that may be necessary for technological access and comfort, and a concise procedure to follow if a citizen suspects or has proof that their privacy has been violated.

[1] http://www.pewinternet.org/Press-Releases/2013/Anonymity-Privacy-and-Security-Online.aspx

2.1.2 Learning outcomes

1. Vulnerable groups will demonstrate knowledge of their rights, understanding of what constitutes a violation of their online privacy, and have a clear idea of where to go for help (a school psychologist or the police) if their rights are violated. Children, domestic violence victims and those exposed to online harassment will belong to this category.
2. Less vulnerable group will seek proper counsel and understand that they are entitled to select the appropriate level of privacy for their individual needs. The digitally reluctant may choose to store little or none of their personal data online, while the handicapped or the elderly may select robust online intervention and assistance (while ensuring that only accredited care-providers have access to that information).
3. General users will demonstrate knowledge of their rights, what constitutes a violation of their online privacy, and have a clear idea of which procedures to follow with respect to a national public authority should they suspect that their rights have been violated.
4. All groups have a heightened awareness about privacy-preserving alternatives to existing technologies and services and how to identify and select them (e.g., in the Internet).

2.2 Practitioners

By practitioners, we refer to those professionals involved in any phase of the lifecycle of an IT system or software that are interested in acquiring the knowledge and skills required to introduce or follow a privacy-by-design approach in their day-to-day work, and also those may be involved in the operation of the resulting system.

We may split practitioners into managerial and development roles. Managerial roles such as Project Managers are responsible for ensuring consistent reporting, risk mitigation, timeline, and cost control for the whole project. Development roles such as analysts, system architects, programmers, testers, etc. are involved throughout the software development process, and deal with the technical details. The name and attributions of these roles may vary depending on the software engineering methodology applied and the context of the project under development.

2.2.1 Practitioners Needs

Among the common learning goals for practitioners we can find:

- To know some of the key terms and concepts involved in a PbD methodology such as e.g. the core principles of a PbD methodology, privacy impact assessment, personal information, privacy enhancing technology, policy, informed consent, anonymity, data minimization, accountability, etc.
- To understand the key aspects of a PbD methodology, and its benefits.
- To have a strong awareness on availability, characteristics, advantages, and disadvantages of different forms of privacy enhancing technologies and understand where they can be applied and the respective trade-offs.

The specific learning goals for managerial roles are:

- To be aware of and understand the legal requirements regarding privacy and how a PbD methodology can help to achieve them.
- To understand what a privacy impact assessment is and its benefits.
- To compile information necessary for introducing a PbD methodology in a software development, producing a plan for implementation.
- To be able to assess the trade-offs and advantages

The specific learning goals for development-related roles are:

- To be able to understand and identify the privacy-related requirements and risks for incorporation into the PbD methodology.
- To be able to carry out a privacy impact assessment.
- To be able to select the correct concept, technique or technology to be applied to a given issue, and apply it in a given context in a correct way.
- To be able to evaluate different alternatives regarding solutions to be adopted to implement a PbD methodology departing from the evidences previously gathered, and decide on its applicability in a given situation.
- To know different and appropriate privacy enhancing technologies in detail to apply them in the different stages of the PbD methodology (design and implementation).

2.2.2 Learning Outcomes

The overall objective of the training material for practitioners is to help them in gaining awareness, understanding and introducing a PbD methodology and corresponding privacy enhancing technologies in their products (systems and software) development.

Specifically, we have identified the following key learning goals:

- Managers: understanding of the need for and benefits of a PbD methodology, its steps, related technologies, and how to produce a plan for implementation.
- Developers: deepened understanding of the technical steps involved in implementing a PbD methodology, as well as the key processes and technologies involved. As a result, they will be able to carry out the different activities required to introduce a PbD approach in a system/software development. For example, carrying out a PIA, identifying the privacy-related requirements, mapping them to technical requirements, selecting the technologies to be applied, integrating and implementing these technologies, etc.
- All: understanding the key concepts underlying a PbD methodology.

Once the previous learning goals have been achieved, the practitioners will be able to effectively apply and/or follow a PbD methodology on their own, as defined by PRIPARE.

2.3 Students

2.3.1 Students needs

The requirements may vary depending on a number of factors such as:

- degree of technicality of the programmes or modules e.g. computing vs. non-computing
- student level e.g. graduate vs. postgraduate
- career goals and directions of students

The following are the identified requirements of student programmes and modules towards understanding and becoming able to apply PbD concepts:

- provide the skills to build privacy and security into IT products and services and consider the trade-offs involved. In particular, the skills to integrate privacy protection and security into the overall engineering lifecycle of such products and services including requirements, design, implementation, and testing phases.
- create an awareness of the privacy-related ethical issues in modern society such as behaviour and location tracking and understand their relevance to PbD.

- provide the skills to cope with privacy issues including identifying and dealing with privacy incidents and mitigating risks in the context of PbD.
- learn the concepts and acquire the skills to conduct privacy and security-related risk assessment, attack surface analysis, threat modelling and compliance reviews to help apply those skills in the engineering of software systems.
- understand background and related technical topics that build the fundament of privacy enhancing technologies or that can affect privacy positively or negatively such as IT-security, human-computer interactions, cryptography, and anonymisation.
- In case of privacy preserving tools and techniques it is important that students learn the capabilities and limitations of these tools and techniques and practice them in a variety of application domains and scenarios e.g. Web services, Android, smart energy.
- understand marketing and business-related considerations of privacy such as the consumer trust and business reputation effects.
- gain insight into legal, societal and ethical issues relating to privacy including national and international regulatory frameworks and mapping these considerations into PbD methodology.
- obtain the skills to build privacy and security technologies that satisfy important requirements of scalability, usability, interoperability, dependability, etc

2.3.2 Learning outcomes

The students who gain the knowledge of the items listed in the learning needs would be able to apply security and privacy by design in different career roles depending on the type of educational programme. The acquired knowledge and skills will apply to development phases as follows:

- Requirements: understanding how to analyse and match general software and system requirements and privacy preserving requirements. This includes identifying conflicts and finding solutions that both deliver business value and protect privacy.
- Design: ability to evaluate design decisions and trade-offs in the management of data in the designed systems including collection and processing restrictions e.g. data minimisation, anonymisation, retention, etc. Learning the consideration of the effect of the evolution and maintenance of the system on privacy. . Students also need to understand how to interface with the users of IT systems in a way that data processing becomes transparent and informed consent becomes possible.
- Testing: ability to test and review based on privacy requirements of both code and runtime functions. Additionally, the ability to consider requirements that are not easy to test.

2.4 Policy and Legal stakeholders

2.4.1 Stakeholders mapping

2.4.1.1 Policy makers and governmental bodies

The category includes anybody who represents a government and exercises public power (legislative or executive). In particular:

- **Policy Makers[2]:** All persons responsible for or involved in formulating policies, especially in politics[3]. The term is perceived includes everybody involved in the policy making (e.g. magistrates[4], lobbyists)
- **Governmental Bodies[5]:** They represent the 'government' and they can either be entrusted with policy making or implementing policy tasks. In particular: The government or any political subdivision, its instrumentalities, any person or organization authorized by law to perform executive, legislative, judicial, regulatory, administrative, military, or police government functions and any intergovernmental organization[6].
- Policy makers and governmental bodies appear in National, European and International level:

a. National level:

· **Ministries:** Justice, any Ministry/Department involved in ICT deployment

· **Independent Supervisory authorities:** National DPA

· **Other**: e.g. in Belgium: Belgian Science Policy Office (Belspo)

b. European Level:

· **European Commission:** DGs: JHA, CNECT, RTD, MARKT, EMPLO etc. / Agencies: FRA, JRC

· **European Parliament:** Committees: LIBE, JURI/ Subcommittees: DROI, AFCO

· **Council of the European Union:** Configurations: JHA Council, TTE Council

· **Independent Supervisory authorities**: EDPS

c. International level

· **International organisations**: UN, OECD etc.

2.4.1.2 Non-Governmental Bodies acting for Human Rights Protection

They are legally constituted corporations created by natural or legal people that operate independently from any form of government[7].

In particular, they are:

· **NGOs:** Statewatch, Privacy International

· **Think Tanks and civil society organisations:** Center for European Policy Studies (CEPS), European Digital Rights (EDRI), La Quadrature du Net etc.

2.4.1.3 Legal professionals: Privacy practitioners (Law Firms, Inhouse Lawyers, DPOs etc.), Professional Associations

2.4.2 Informational Needs

In order to define informational needs of policy makers, governmental and non-governmental bodies, it is necessary to define the knowledge patterns of the target group. It is assumed that

[2] http://www.adamsdrafting.com/defining-government-body/

[3] Oxford Dictionary,"Policy Maker", http://www.oxforddictionaries.com/definition/english/policymaker

[4] Judicial power is the third component of the sum of public power and, as in the case of the others, is constitutionally separated from the executive and legislative powers. It should be taken into account that CJEU has functioned as a 'de facto' policy maker of the EU. (See Hjalten Rasmussen, Hjalten, On Law and Policy: In the European Court of Justice, Martinus Njihoff Publishers 1986)

[5] http://www.oxforddictionaries.com/definition/english/policymaker

[6] Ken Adams, "Defining "Government Body", August 2009, http://www.adamsdrafting.com/defining-government-body/

[7] Wikipedia, "Non-governmental Organisaton", http://en.wikipedia.org/wiki/Non-governmental_organization

there is at least general knowledge of the field of privacy law/technologies. There have been identified 3 knowledge patterns that illustrates quite diverse stakeholders profiles:

- Even though there is an overall privacy-awareness, the majority of the target group does not possess specific knowledge on PbD.
- Parts of the target group specialise in law, technical and/or political sciences but lacks input in the other disciplines accordingly.
- Parts of the target group might possess specific overall knowledge on privacy and PbD but it is up to its interest to follow the latest developments and stay up to date.

The informational needs of the target group should build up on the existing knowledge pattern on the basis of the purpose and the use that is intended from each member of the target group. They have been classified as follows:

a. **Policy makers acting in normative level** (formulating policy):

   Privacy could be seen as a means to effective policy making. In the Commission Impact Assessment Guidelines[8], privacy is a requirement that should be taken into account in the EU policy making process. However, this is not always the case. Policy makers acting in normative level are sometimes unaware of the privacy risks stemming from the policies they develop in several policy fields. Thus, their needs could be described as follows:

- Need of general knowledge on PbD to take into account in a broad range of policy fields.
- Specific knowledge in the field about points of struggle/ of discussion in the field with an impact on the normative or operational framework[9].

b. **Governmental bodies active in operational level** (when implementing policy):

- Specific knowledge: when issuing a tender, they need to issue system specifications that include privacy by design and privacy by default principles. There is need for operational knowledge; in other words, how to apply the normative framework.

c. **Non-governmental bodies active in the field of human rights (activists**): They are interested in the same level of knowledge as a., as they aim at lobbying in a level playing field.

d. **Legal professionals:** They already know about the general privacy legal framework but they need specific training on PbD in order to implement it for the development of new products and services. They might be interested in the same level of specific knowledge as a., in order to represent the rights of their clients before the court or policy makers or to apply it in their organization.

2.4.3 Learning Goals

1. To gain an overall understanding of the main privacy issues: to be able to recognise and recall key concepts (personal data, consent, PbD, SbD, Privacy by Default, Accountability, PIA, PETs, privacy risk, lifecycle data protection management etc) and legal principles: data minimization, purpose limitation, proportionality etc. To understand the legal framework for privacy (Draft regulation) and be able to relate it to

[8] European Commission, "Impact Assessment Guidelines" SEC(2009) 92, January 2009

[9] When an authority has the discretion to publish a tender, vote for or decide on the requirements, criteria etc., it formulates policy in the executive level. In case there is no discretion to act but the authority follows an order, it implements policy in the executive level.

their work. To know and be able to assess critically certain PbD-friendly technologies and policy areas they can be applied.

2. To gain specific understanding of the concept of Privacy by Design (context and examples) and link it to their work.
3. To be able to approach privacy from a risk management perspective: to be able to identify threats to privacy and privacy requirements in a certain project in different settings. To be able to recognise and assess in high-level PbD methodologies that have been followed in certain projects.
4. To be aware of useful information sources when looking for specific material.

2.5 Material reuse

In order to address the needs of stakeholders as described in sections 2.1-4, we will conceive structured and targeted educational and informational material.

Wherever possible we will aim at reusing, and integrating within the structure of our educational material, existing material already made available by the EU (e.g. Justice: data-protection web pages) and other organisations.

Furthermore, when ever possible, we will aim at designing modules (units of content) that are directly reusable by, or easily adaptable to, various stakeholders. Ideally, courses and trainings can be directly composed by selecting a set of complementing modules, ordering them appropriately, and configuring the modules to fit the necessary level of detail for the target group. The later is relevant as a specific module (e.g., legal framework or PETs) needs to be adjusted to the target group and will have to be presented in varying level of detail. Ideally, modules directly allow this customization by activating or deactivating specific content or choosing alternatives. In some cases, material for different groups may be so heterogeneous that completely different instantiations of a module need to be provided.

3 Identification of Existing Material

This will complement the more specific PbD literature review done in task 1.1

3.1 Online resources and publications

This section provides a breakdown of the current resources and publications available online regarding privacy, how they are presented, and their relevance to each of the four stakeholders. The material can be classified into the following types:

- Introductory readings
- Usability studies
- Users' studies
- Regulation
- Privacy issues with specific tools and practices or in specific environments
- Tools to verify privacy
- Tools for privacy protection and PET
- Technology issues
- Reference sites
- About privacy statements and use conditions

The introductory readings cover a broad range of topics and issues around privacy and are relevant to all stakeholders. An example of an introductory reading is Ann Cavoukian's *Surveillance, Then and Now: Securing Privacy in Public Spaces*[10] or the Electron Frontier Foundation's *Who has your back? Third Annual Report on Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data*[11]. The usability studies section contains past studies that have been conducted to assess various aspects of privacy. Studies in this section would be, for example, those presented at the Symposium On Usable Privacy and Security such as *Little Brothers Watching You: Raising Awareness of Data Leaks on Smartphones*[12] by Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Cranor, and Carolyn Nguyen. The information available in usability studies is most relevant to the student and practitioner stakeholders. The user's studies section consists of studies by governmental and non-governmental bodies. One example of a user study is the *Attitudes on Data Protection and Electronic Identity in the European Union*[13] study conducted by TNS Opinion & Social. User's studies are most appropriate for practitioners and policy makers. The regulation section includes resources regarding regulatory recommendations/resolutions, unofficial regulatory proposals, court rulings, statements supporting rulings, and academic literature. The contents in the regulation section are apposite to all four of the stakeholder groups. The section regarding privacy issues with specific tools and practices or in specific environments consists of resources covering topics from people search websites and Facebook, to web cameras, radio frequency identifiers (RFIDs), and eye tracking. Specific environments include: medical, work, school, public transport, and smart spaces. Each of the stakeholders can benefit from the resources in the privacy issues with specific tools and practices or in specific environments

[10] http://www.privacybydesign.ca/index.php/paper/surveillance-then-and-now-securing-privacy-in-public-spaces/
[11] https://www.eff.org/who-has-your-back-2013
[12] http://research.microsoft.com/apps/pubs/default.aspx?id=194401
[13] http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

consists section. The tools to verify privacy and tools for privacy protection parts provide a list of several tools currently available online. It is important to note that not all of the tools have been tested; the fact that they are listed here does not constitute a recommendation. An example of one of the tools to verify privacy is Panopticlick, which tests the user's browser to see how unique it is based on the information it shares with the sites it visits. An example of a tool for privacy protection is the Tor project, which offers protection against traffic analysis. Both sections are relevant for all four of the stakeholders. The technology issues category consists of material covering known technological issues, such as Peter Fecklessly's *How Unique Is Your Web Browser?*[14], and is important for the student and practitioner stakeholders. The reference sites section is a collection of reference sites, associations, and conferences on privacy. The *Privacy by Design*[15] site of the Information and Privacy Commissioner of Ontario is an example of an item under the reference sites section. Another example is the *World Privacy Forum*[16]. This section is useful for the general public, students, and practitioners. The about privacy statements and use conditions section consists of some privacy statements and conditions of use (for example, *Amazon.co.uk conditions of use and sale*[17]), as well as a free privacy policy generator application called *AppPrivacy*[18]. This section is relevant to all stakeholders.

The majority of the information is presented in a text based format, such as a website, online article, or online paper. Others modes of presentation are video, information graphics, and in one case an interactive game.

3.2 Courses

Definitions:

- Module: unit of contents, typically lasting from a few minutes to a few hours
- Course: unit of delivery normally organised in a sequence of lectures over a quarter or semester
- Stream: a sequence of related courses or modules, usually taken in successive semesters and normally leading to a specialization within a major
- Programme: course of study, typically leading to an award such as a degree or diploma (major/minor).

In the text below **G** indicates Graduate courses/programmes/etc. and **U** indicates Undergraduate courses/programmes/etc.

3.2.1 Programs in Privacy for CS/ICT student (both G and U)

In recent years, a few educational institutes have begun to offer programmes geared specifically towards Privacy for CS/ICT students. The undergraduate programmes are generally 4-years long and the graduate programmes are 1 to 2-years. Over the period of the programme, students participate in a set of required core courses along with several electives that help the students gain both practical and theoretical knowledge in privacy.

[14] https://panopticlick.eff.org/browser-uniqueness.pdf
[15] http://www.privacybydesign.ca/
[16] http://www.worldprivacyforum.org/about-us/
[17] http://www.amazon.co.uk/gp/help/customer/display.html?nodeId=1040616
[18] http://www.appprivacy.net/#generate-policy

Currently, the programme with the highest degree of focus in privacy is the Master of Science in Information Technology – Privacy Engineering at Carnegie Mellon University. The programme teaches privacy engineering skills for jobs in industry and government. The core courses for the programme are:

- Information Security and Privacy
- Privacy Policy, Law, and Technology
- Foundations of Privacy
- Law of Computer Technology
- Usable Privacy and Security
- Engineering Privacy in Software
- Management of Software Development for Technology Executives

Additionally, over the summer the students work in small groups on the Privacy-by-Design Capstone Project[19], a "learning-by-doing component" of the program that enables the students to take on the role of a privacy consultant on a team project and gain first-hand experience.

Another programme specializing in privacy is the Information Security and Privacy specialisation of the Security and Privacy Major provided by European Institute of Innovation and Technology. The two year programme "aim[s] to provide students with an understanding of the concepts and technologies for achieving confidentiality, integrity, authenticity, and privacy protection for information processed across networks". The courses specific to the Information Security and Privacy specialisation are:

- Information Security and Privacy
- Privacy Enhancing Technologies
- Formal Methods in Information Security and Privacy
- Practical Aspects of Information Security
- Seminar on Selected Topics in Information Security and Privacy

Similar to the Privacy Engineering Master's, the students are given an opportunity to gain first-hand experience through an internship in the industry or with a research centre.

3.2.2 Programs in Privacy for Other students (both G and U)

3.2.3 Courses in Privacy for CS/ICT student (both G and U)

This section provides an overview of what is involved in current and past courses in Privacy. The courses are designed for CS/ICT students and range from a graduate to an undergraduate level. The section is separated into the following units: topics addressed, presentation and term paper topics, pre-requisites, and recurring or predominant material.

There are a number of topics addressed by courses in Privacy that span multiple areas of CS/ICT as well as other fields. The topics have been extracted from previously taught courses and are presented here in a broad fashion so as to illustrate the possible content involved in each topic. It should also be noted that privacy-related topics are often taught as part of broader IT

[19] http://privacy.cs.cmu.edu/capstone/index.html

security courses. Where no dedicated privacy courses are available, this WP should also aim for allowing a module extension of an IT security course.

The topics addressed are as follows:

- *Definitions of Privacy* – Privacy from different perspectives, such as technological, ethical, legal, and economic
- *Internet privacy* – Search engines, social networks, HTTP cookies, Internet service providers, device fingerprinting, etc. (see for example, *Sensitive Information in a Wired World*[20], *Security Privacy and Trust*[21], *Societal Impact of Information Technologies*[22])
- *Databases* – The different definitions, techniques, issues, and algorithms for achieving privacy within stored data. (For example see, *A Study of Perturbation Techniques for Data Privacy*[23])
- *Location Privacy* – Technical approaches, incentive-models for encouraging privacy, and economic models to privacy on devices with location-based services. (For example see, *Local Data and User Privacy*[24], *Security and Privacy in Mobile Systems*[25])
- Privacy-Enhancing Technologies – technological approaches to privacy protection. This overlaps to some extend with Internet and DB privacy and is an orthogonal view on the topic. For examples see, *Privacy Seminar Radboud University Nijmegen*[26].
-

Professor Antonio Kung, a member of PRIPARE, is currently teaching a course called 'Security, Privacy, and Trust' at the American University of Paris. The course is designed to provide students with an understanding on the need for security, privacy and trust in ICT. Both legal and ethical aspects are covered in the course as well. Technology for security, privacy and trust is presented at a functional level. The following topics are covered: security threats and solutions, intellectual property rights, anonymity and identity, business stakeholders privacy obligations, privacy in today applications (search engine, social networks, location oriented services, RFID-based applications), privacy enhancing technologies, privacy policy enforcement, trusted computing. The learning objectives for the students are to learn the fundamental concepts related to security, privacy and trust: today security threats and solutions from a user point of view, the various perceptions of privacy and existing privacy enhancing technologies from a user point of view, the meaning of trust in ICT and trusted computing solutions from a user point of view.

During the individual courses, it is common to have students give presentations and or submit a term paper covering a selected topic. For example, in a course on Internet privacy some possible presentation subjects include methods of creating anonymity, protocol design for preserving privacy, or a digital-cash system like BitCoin. A course on databases and privacy may include topics such as cryptography in data mining, data collection algorithms that address privacy, or synthetic datasets.

[20] http://zoo.cs.yale.edu/classes/cs457/fall13/
[21] http://www.aup.edu/academics/course-catalog/cs2055/spring-2014
[22] http://m.stevens.edu/academics/course_desc.php?course_id=3105&prog_id=45
[23] http://theory.stanford.edu/~nmishra/cs369-2004.html
[24] http://www.cs.umd.edu/class/spring2012/cmsc818c/
[25] http://www.uni-ulm.de/in/vs/teach/spms.html
[26] http://www.cs.ru.nl/~jhh/secsem.html

Courses covering advanced topics or involving specialized technical skills often have pre-requisites that the CS/ICT student must fulfil before taking the course. A course focusing on the technical challenges of handling sensitive data can require a student to have previous experience in cryptography or a basic understanding of information technology security (see for example, *Privacy in a Networked World*[27]). Additionally, courses concerning location privacy can require a level of understanding of various networks such as mobile or peer-to-peer and a background in probability, statistics, cryptography, and algorithms are helpful for statistical database courses (e.g. see, *Local Data and User Privacy*[28]).

The material on Privacy currently presented to CS/ICT students varies by the course, instructor, and school. However, there are authors and texts that appear more frequently than others in CS/ICT courses in Privacy. The list below has been compiled from courses' reading lists:

Authors:

- Daniel Solove
- Simon Garfinkel
- Helen Nissenbaum
- Lorrie Faith Cranor

Texts:

- Daniel Solove's "I've Got Nothing to Hide' and Other Misunderstandings of Privacy"
- Daniel Solove's "A Taxonomy of Privacy"
- Simon Garfinkel's "Database Nation"
- Microsoft's "Privacy Guidelines for Developing Software Products and Services"

3.2.4 Socio-Ethical and Legal courses

The following section is meant to provide an overview of current and past courses that approach privacy from a socio-ethical and or legal perspective. The courses are each a semester in length and range from the undergraduate to graduate level. The section is separated into the following units: topics addressed, pre-requisites, and recurring or predominant material.

The following topics were compiled from multiple socio-ethical and legal courses in privacy:

- *Definitions of privacy* – Privacy from a philosophical, ethical, legal, and economic stand point.
- *Policies on privacy* – The role of policies in technology and the issues related to privacy (See for example, *Privacy Policy, Law, and Technology*[29], *Privacy in the Digital Age*[30])
- *Social impact of technology* – How technologies such as social networks, big data, and smartphones impact society (See for example, *Privacy Versus In-Your-Face Big Government*[31], *Social and Ethical Issues in Computing*[32])

[27] http://www.stevens.edu/compsci/graduate/masters/courses/viewer.php?course=CS578&type=syl
[28] http://www.cs.umd.edu/class/spring2012/cmsc818c/
[29] http://cups.cs.cmu.edu/courses/pplt-fa13/
[30] http://master.econ.uni-freiburg.de/students/courses/1prof._acquisti_syllabus.pdf
[31] http://doubletap.cs.umd.edu/purtilo/239R/
[32] http://cs.unm.edu/~pgk/293f13/

- *Cross-Cultural privacy* – Laws, regulations, and cultural differences at a global level (See for example, *Privacy Policy, Law, and Technology*[33], *Information Ethics*[34])
- *Biometrics* – The challenges, opportunities, and issues biometrics raises (See for example, *Privacy Policy, Law, and Technology*[35])
- *Sociotechnical Computer Ethics* - Major ethical theories and frameworks that have shaped the field of information ethics (See for example, *Information Ethics*[36])

The undergraduate level courses are generally open to all students and do not have any pre-requisites. The graduates require a certain level of knowledge in the course topic due to the depth of the material studied (See for example, *Privacy Policy, Law, and Technology*[37], *Privacy in the Digital Age*[38]).

3.2.5 Certification courses for practitioners

This section provides an overview of programs that lead to a professional certification in the privacy domain. The courses are designed for practitioners, with different roles, who want to demonstrate understanding of different privacy aspects and skills to develop privacy-compliant systems and software. The section is separated into the following units: topics, intended audience, pre-requisites, and material.

The following topics have been gathered from different privacy-related certification programmes (See annex 6.6 Certification Programs for Practitioners for details):

- *Introductory aspects* – Privacy, why it matters to a company, legal considerations.
- *Technical aspects* – Introduction to different issues related to privacy and technologies/products that may contribute to tackle them e.g. Graphical User Interfaces, Identity and Access Management, Privacy Enhancing Technologies, hardware protection, etc.
- *Management aspects* – Realizing a privacy-aware company, which includes creating a company vision, creating and training a privacy team, communicating to stakeholders, defining privacy policies and processes, and developing and implementing a privacy program.
- *Domain-specific aspects* – Legislation and industry standards focused on specific domains e.g. healthcare industry.

The certification programs are aimed at managerial roles, development ones, or a mix of them. For example, the Certified Information Privacy Professional/Information Technology (CIPP/IT)[39] targets professionals who are responsible for the development, engineering, deployment and/or auditing of IT products and services. On the other hand, the Certified Information Privacy Manager (CIPM)[40] addresses managerial roles who are responsible for privacy at any

[33] http://cups.cs.cmu.edu/courses/pplt-fa13/
[34] http://homes.soic.indiana.edu/nensmeng/courses/i453ethics.html
[35] http://cups.cs.cmu.edu/courses/pplt-fa13/
[36] http://homes.soic.indiana.edu/nensmeng/courses/i453ethics.html
[37] http://cups.cs.cmu.edu/courses/pplt-fa13/
[38] http://master.econ.uni-freiburg.de/students/courses/1prof._acquisti_syllabus.pdf
[39] https://www.privacyassociation.org/certification/cipp_certification_programs/cipp_it
[40] https://www.privacyassociation.org/certification/cipm_certification_program

level of their organization. Finally, some are focused on professionals within a specific domain, for example, the healthcare industry (See for example, Certified in Healthcare Privacy and Security [41]).

The general certifications programs are open to practitioners in the domain and do not have any pre-requisites. The programs focused on the healthcare domain require between 2 and 8 years of experience in the knowledge area of the credential, which includes security, compliance and privacy in the healthcare industry.

The material used by these certification programs includes textbooks, online training, preparation in-site classes, and other reference material such as papers on the topic and guidelines by privacy authorities.

3.3 Reference material for policy makers, governmental and non-governmental bodies

3.3.1 From the EU

3.3.1.1 Legislation with references to Privacy by Design:

I. **The draft Regulation of the European Parliament and the Council on the protection of the individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation)** adopts officially the principle Privacy by design. Even if it is referred as data protection by design for the purposes of the regulation, its content should be understood as covering privacy as a comprehensive concept. Article 23 requires that privacy should be embedded in the whole lifecycle of data management and this should be ensured by procedural safeguards. As a further specification of privacy by design is the principle privacy by default.

II. **The draft Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data also adopts the principle privacy by design.** Article 19 explains that technical and organisational measures and procedures shall be pursued to ensure thee compliance with the principle.

III. **The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such** data does not explicitly refer to privacy by design. However, there are elements implying it. In particular the directive calls for technical and organizational measures to ensure secure data processing at the stage of design as well at the stage of operation of ICT.

[41] http://www.ahima.org/certification/chps

3.3.1.2 Other privacy-relevant legislation

I. **The Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)** requires telecoms operators and Internet service providers to keep personal data confidential and secure. In cases of personal data breaches, the provider has the duty to report them to a specific national authority and inform the concerned subscriber directly, when the breach is likely to adversely affect personal data or privacy.

II. **The Directive 2006/24/EC of the European parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC** provides that telecommunications data shall be stored for 6-24 months stipulating a maximum time period. Law enforcement authorities have the right to request access to details such as IP address and time of use of every email, phone call and text message sent or received. Permission for such access can be only granted by court.

III. **Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data** requires that the EU institutions and bodies ensure fair and lawful processing of personal data. Processing and storage of data should be performed in a way that respects the principles of data minimization, purpose limitation, legitimate interest and proportionality.

3.3.1.3 Opinions with references to Privacy by Design:

3.3.1.3.1 EDPS

The EDPS as an independent supervisory authority provides guidance to the EU institutions and bodies on data protection issues and has generally endorsed the principle of PbD. It has often referred to the principle as follows:

- **EDPS, The EDPS Video-surveillance Guidelines of March 2010.** As pointed out by the EDPS "*the objective of the Guidelines is to offer practical guidance to the European Union Institutions and Bodies operating video surveillance equipment on how to comply with the regulation and use video-surveillance responsibly with effective safeguards in place".* The Guidelines approach PbD within the context of video-surveillance. They concentrate on addressing data protection issues at the very beginning, which means amongst others, building privacy into the system, use of PETs and performance of privacy impact assessments. (specific material on PbD in the domain of video-surveillance)[42]

[42] https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf

- **EDPS, Opinion of the 16 October 2010 on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, OJ C 280/01.** The opinion identifies the insufficient deployment of PbD in ICT and endorses its further application as a guiding principle of Digital Agenda through legal instruments. It recognizes its tremendous potential to enhance individuals' trust on ICTs but also identifies RFID, social networks and browser applications as areas of specific concern. (specific material on PbD in the ICT domain in general)[43]

- **EDPS, Opinion of the 17 November 2009 on the Communication from the Commission to the European Parliament and the Council on an area of freedom, security and justice serving the Citizen, OJ C 276/02.** The opinion presents PbD as a response to the need for privacy and personal data protection in a context of increasing exchanges of personal data. Needs for further legislative and non-legislative actions to improve the framework for data protection are identified. The EDPS finds a legal obligation for builders and users of information systems to use systems which are in accordance with the principle of privacy by design. (general material on PbD in the domain of freedom, security and justice)[44]

3.3.1.3.2 Article 29 Working Party

The article 29 of the Directive 95/46/EC provides for a Working Party to give opinions on several issues concerning the application of privacy related legislation and addresses national policy makers as well as EU policy makers. In particular, it is entitled to examine questions regarding the uniform application of the national measures adopted, to provide the Commission opinions on the level of protection in the Community and in third countries, to advise the Commission on possible legislation amendments, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms (article 30).

- **Article 29 Data Protection Working Party and Working Party on Police and Justice, The future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP 168, December 2009).** This contribution mentions that privacy by design is not entirely new as a concept, as the directive 95/46/EC called data controllers to implement technology safeguards in the design and operation of ICT. It also recognises that the application of such principle would emphasize the need to implement privacy enhancing technologies, 'privacy by default' settings and the necessary tools to enable users to better protect their personal data. Finally, it foresees the need for adoption of further sector specific regulations to apply the principle in several contexts. (Specific material on PbD)[45]

- **Article 29 Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications**

[43] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:280:0001:0015:en:PDF
[44] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:276:0008:0020:EN:PDF
[45] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

(WP180, February 2011). In this opinion the working party analyses the proposed PIA framework and amongst others sees PIA as a tool able to promote privacy by design, which enables addressing privacy and data protection before a product or service is deployed. (General reference to PbD as relevant to the PIA Framework on RFID)[46]

- **Article 29 Working Party, Opinion 12/2011 on smart metering (WP183, April 2011).** In this opinion, the article 29 Working Party encourages the adoption of default settings for smart meter. The aim is to preserve consumers' privacy during processing of meter readings, and in particular regarding collection, storage, and transmission of data. Technical specifications of the system shall ensure privacy by design and privacy by default, enhancing user control over the processing of his data. (Specific material on PbD in the field of smart metering)[47]

- **Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies (WP193, April 2012).** In this opinion the working party recognises the need for data controllers to realise the privacy risks stemming from the processing of biometric data and to implement Privacy by Design. It also clarifies that the requirement for privacy by design concerns the whole value chain of biometric systems: manufacturers, when they design biometric systems, integrators and resellers, when they define biometric systems as final products and clients, when they request specific technical features of biometric systems. (Specific material on PbD in the field of biometric technologies)[48]

- **Article 29 Working Party, Opinion 02/2013 on apps on smart devices (WP202, February 2013).** The opinion suggests that manufacturers shall embed privacy and data protection in the mobile devices or application systems from the very beginning of their design. It also states that Privacy by design is explicitly required for the design of telecom equipment, as provided under the radio and telecom terminal equipment directive. (General reference to PbD as relevant to the field of smart devices)[49]

- **Article 29 Working Party, Opinion 06/2013 on open data and public sector information ('PSI') reuse (WP207, June 2013)**. In this opinion the working party proposes that the public sector body should perform a thorough PIA before opening data for re-use and points out the importance of PIAs to comply with the principle of privacy by design. (General reference to PbD as relevant to the proposed framework)[50]

[46] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf
[47] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf
[48] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf
[49] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
[50] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf

3.3.2 From countries other than EU

3.3.2.1 Data protection authorities outside the EU

The information and privacy commissioner of Ontario, Canada, as a pioneer working on Privacy by Design, has managed to create a long list of material. It provides general and specific material on how the principle should be interpreted, and applied in several different fields. More information can be found here: http://www.privacybydesign.ca/ A few examples are worth mentioning:

- **Ann Cavoukian, Privacy by Design in Law, Policy and Practice. A White Paper for Regulators, Decisions-makers and Policy-makers, Information and Privacy Commissioner, Ontario, Canada, August 2011.** The white paper includes a comprehensive introduction on the legal concept of Privacy by Design. It further focuses on organizational and regulatory approaches able to incorporate the principle in data management processes of an organization. Finally, it provides a list of examples illustrating how it can fit in a legal framework. (specific material on PbD)[51]

- **Ann Cavoukian, Scott Taylor & Martin E. Abrams, Privacy be design: Essential for organizational accountability and strong business practices, Identity in the Information Society, (Springer, 2010), 405-413.** This article illustrates how Privacy by Design can be integrated in accountable business practices. It provides examples how to design organizational controls that build accountability and privacy in business processes and thus enhances consumers' trust.(specific material on Privacy by Design)[52]

3.3.2.2 Other material

- Initiative of the American Think Tank **'Future of Privacy'** to compile material in order to raise the awareness of policy makers on current and emergent privacy issues. In yearly basis, a compilation of scientific papers including research and analytical work on a variety of privacy topics takes place after a relevant call for papers. In particular, the papers propose achievable short-term solutions or new analytical tools for medium/long-term solutions. For 2013, selected topics were: digital market manipulation, face recognition and biometric data privacy, benefit cost analysis in digital privacy debates, FTC privacy jurisprudence, cloud computing, metadata, privacy by design and obscurity by design, EU vs US on personal information, constitutionality of privacy law. (Material on specific privacy issues and some specific material on PbD)[53]

[51] http://www.ipc.on.ca/images/Resources/pbd-law-policy.pdf
[52] http://download.springer.com/static/pdf/762/art%253A10.1007%252Fs12394-010-0053-z.pdf?auth66=1391260916_dfdd27565d0af5b0c1325308387e499f&ext=.pdf
[53] http://www.futureofprivacy.org/privacy-papers-for-policy-makers/

4 Specification of Material for each type of stakeholder in modular structure

The proposed educational material will address a set of themes for each stakeholder. The themes are organised by *general knowledge* and *specific knowledge*. As a rule of thumb, modules about general knowledge may be reused across stakeholders, where specific knowledge may only be useful for a specific set of stakeholders.

4.1 Summary of themes for the production of educational material

4.1.1 Themes for general public

General knowledge:

- Awareness
  - Dangers of privacy violations
  - Rights: what constitutes a violation of privacy (Data Protection Directive 95/46/EC, proposed EU Data Protection Regulation, Seven types of privacy)
  - The role of Privacy by Design in privacy protection
- Action
  - What to do in case of privacy infringement (governmental and non-governmental organisations)

Specific knowledge:

- PbD in specific contexts
- Tools for privacy protection
- Risk management (risk assessment, what actions can be taken, what tools are available)

4.1.2 Themes for practitioners

General knowledge:

- **Privacy-by-design principles and concepts**

Specific knowledge:

Among the steps of the methodology, we may include the following themes:

- **Privacy context**. The legal context as a source of privacy requirements for a software development process. This material can be reused from Legal Practitioners general knowledge part.
- **Risk management.** What it is and its benefits for a software development process. Privacy Impact Assessment as a risk management methodology applied to PbD.
- **Best practices.** Explanation of best practices to realize a PbD development. Privacy patterns as an example of a best practice: What a privacy pattern is, how to understand them, and case studies demonstrating how to apply them.
- **Technologies and solution for implementing PbD.** From an overview of different technologies useful for fulfilling privacy requirements, to a deep explanation of some of them.
- **Testing and validating the outcomes of the PbD process.**

Other specific knowledge would include

- **Privacy Patterns**
- **Privacy Failures**
- **Privacy Design Strategies**
- **Location Privacy**
- **Anonymous Cash**

4.1.3 Themes for students

General knowledge:

- Privacy in ICT environments

Specific knowledge for CS/IT students:

- Privacy Enhancing Technologies
- Privacy in ICT environments
- Database Privacy
- Cloud Privacy
- Mobile Privacy
- Economic Aspects
- Privacy risks and incidents

Specific knowledge for non-CS/IT students:

- History of technology and regulation relevant to PbD
- Principles and processes of PbD
- Application of EU privacy law online
- Technology responses to privacy problems

4.1.4 Themes for policy and legal stakeholders

General knowledge:

- Existing Legal Sources: Data protection Directive, E-Privacy Directive, Data Retention Directive, Regulation for Data Protection in EU Institutions
- Basic principles: consent principle, data minimization (proportionality), data quality, purpose specification/limitation, transparency, user's right of access/right to object, confidentiality and security of processing, obligation to notification, data retention, right to erasure
- Data protection reform: 2 drafts: General Data protection Regulation, Data protection Directive for the processing of data by law enforcement authorities, major changes

Specific knowledge:

- Part I: Context. The concept of Privacy by design.
    - How did the concept develop? (context) PbD, PETs, Europrise seal, etc.

- How PbD is implemented in the draft regulation? (broader view - Privacy by Design, by Default, Accountability, PIA, privacy risk management, how data minimisation is reinforced in the draft regulation?)

- Part II: How legal principles affect the design process.
  - Privacy risk management: data governance/ PIA/privacy risk management methodologies
  - Examples: Privacy by design in the field of cloud computing and biometric verification in border control
- Part III: How legal principles affect policy making.

4.2 Tabular overview of modules

The tables below summarise the modules that will be produced during the course of the project. Each row contains the subject area addressed, the main stakeholder for the module, the module name, the mode of presentation, the expected time of delivery, and the contributing partner of that module. The following sections 4.3-6 describe the material in further detail and Appendix 2 contains a version of the tables also including a brief description of the content of each module.

General Public		
Subject	Module	Mode of presentation
Dangers of privacy violations and privacy rights	Smart use of smart devices	short fiction film
	A Day in the Life of Max	Infograph
	The PbD game	board game for children
	Do you feel observed?	printed brochure
Privacy by design in privacy protection	The PbD test	Web page
	The PbD cartoon	cartoon for children
PbD in specific contexts	Work	Infographic/brochure
	School	
	Transport System	
	Smart spaces	
	Medical records	
Tools for Privacy Protection	TOR	Slides
	Blocking ads	Infographic/brochure
	Managing Privacy Settings	
EU Legal Order	Existing legal sources	Slides + reading material

IT Practitioner		
Subject	Module	Mode of presentation
PbD methodology, PRIPARE	PRIPARE principles and concepts	Slides + select reading material
	PRIPARE methodology: Overview	
	PRIPARE methodology: Privacy requirements engineering.	
	PRIPARE methodology: Privacy impact assessment and risk analysis	Slides + select reading material, templates, and examples of use
	PRIPARE methodology: Best practices	Slides + select reading material, templates, examples of use, and a catalogue of best practices
Privacy Patterns	privacy patterns	slides
Privacy Motivation	Failures in Privacy Systems	Slides, references to articles
Privacy Strategies (see Hoepman[54])	Minimise	slides, exercises
	Hide	
	Separate	
	Aggregate	
	Inform	
	Control	
	Enforce	
	Demonstrate	
Location Privacy	Location privacy	slides, exercises
	Privacy in transport systems	slides, exercises
Anonymous Cash		slides, exercises

[54] Hoepman, Jaap-Henk. "Privacy design strategies." (2012) http://arxiv.org/pdf/1210.6621.pdf

Students		
Subject	Module	Mode of presentation
CS/Engineering Students		
PET	Privacy Enhancing Technologies and limitations	Reading list, pointers to existing material
Privacy in ICT environments	Understanding privacy	Reading list, + existing material,
	Privacy in the Internet of Things	Slides, exercises, reading list
	Privacy enhancing techniques for Web Services	Slides, exercises, reading list
	Secure programming	
	Security and privacy in software engineering	
	Web security and vulnerabilities	
	Cryptography	
	Security vs. privacy	Slides, exercises, reading list, pointers to existing material
	Anonymisation	Pointers to existing material, text, video
	Security and privacy patterns	Slides, exercises, reading list, pointers to existing material
Database Privacy	Cryptography	Slides, exercises, reading list, pointers to existing material
	Web and database security and vulnerabilities	
	Privacy preserving data management	Reading list, pointers to existing material
PbD Privacy risks and incidents	Security management	Slides, exercises, reading list, pointers to existing material,
	Privacy Impact Assessment (PIA)	Pointers to existing material
	Compliance reviews	
Cloud Privacy	Cloud privacy patterns and best practices	Slides, reading list
Mobile Privacy	Privacy issues in mobile devices	Pointers to existing material
	Privacy vulnerabilities and solutions in Android	Slides, examples and exercises
Economic Aspects	Trust and reputation	Slides, reading list, pointers to existing material
NON-CS/Engineering Students		
History leading to PbD	History of technology related to PbD	Slides and exam questions
	History of Human Rights related to PbD	Slides and exam questions
Principles and processes of PbD	PbD: principles, processes, and operationalization	Slides and exam questions
Application of EU privacy law online	EU regulation and privacy	Slides and exam questions
Technology responses to privacy problems	PbD: perspectives and limitations	Slides and exam questions

Legal and policy stakeholder		
Subject	Module	Mode of presentation
Data Privacy	Basic principles/ Relevant legislation	Slides + reading material
Data Protection	Data protection reform	
PbD,: context	Part 1: How did the concept develop?	
	Part 1: How is PbD implemented in the draft regulation?	
PbD,: design process	Part 1: Privacy risk management: data governance/ PIA/privacy risk management methodologies	
	Part 2: examples	
	Part 3: How do legal principles affect policy making?	

4.3 General Public

The following educational material is designed (1) for the general public, (2) for the most vulnerable members of society, and (3) for those who are not digitally connected (the digitally reluctant), but remain exposed to privacy violations. Due to the heterogeneous nature of the term General Public, we have included a range of both visual and text materials in order to reach as broad of an audience as possible.

4.3.1 General knowledge:

A first set of material addressed the dangers of privacy violations and privacy rights:

- General Public: the mode of presentation to the general public will be primarily visual, and will include a short fiction film on the dangers of privacy violations during the use of smart devices, as well as an infographic on A Day in the Life of Max featuring 8 typical privacy violations that we all encounter.
- Most Vulnerable: the mode of presentation is in the form of a board game for children explaining their right to privacy and how their rights may be violated in ways that threaten their safety.
- Digitally reluctant: a printed brochure that could be made available at banks and medical offices explaining what happens to citizens' private information, even if they do not use digital tools, for example, and believe that they have nothing to hide.

A second set concentrates on the role of Privacy by Design in privacy protection:

- General Public: the mode of presentation will be an online information page that informs users of how they may control their online information and retain confidentiality. Users will be required to make a range of privacy choices in order to use the page.

- Most Vulnerable: the mode of presentation is in the form of a cartoon for children which explains the basic tenets of privacy by design and what sort of embedded privacy choices they should look for when online.
- Digitally reluctant: a second printed brochure explaining the key concepts of privacy by design and its role in privacy protection for all citizens.

Action: All tools will indicate the address of the National Data Protection Office, and suggest that citizens who believe that their privacy has been infringed contact either the National Data Protection Office or, in the case of children or the digitally harassed, the police.

4.3.2 Specific knowledge

The materials under this rubric will be designed for the adult general public that wishes to learn more about Privacy by Design.

PbD in specific contexts - For each one of the following contexts we will develop information material about privacy threats and how PbD may support fostering a risk management culture, together with best practices for the management of incidents. The material will be in the form of infographic, FAQ sheets, and brochures with references to online resources.

- At work
- At School
- Transport system
- Smart spaces
- Medical records

Tools for privacy protection – This material will provide advice and reports of user experience with the use of various tools for privacy protection and will include:

- Tor: An overview of the Tor project, including its origin, evolution, how it works, what it protects, its limitations, and possibilities.
- Blocking ads: Which tools allow limiting the collection of data while browsing and reducing advertising
- Managing Privacy Settings: Focussed on social networks

Risk management: All tools will indicate how to assess risk and what actions can be taken in case of incidents.

4.4 Practitioners

The material for practitioners will contain two modules. The first one is general knowledge aimed at introducing the PRIPARE principles and concepts, while the second one provides specific knowledge providing technical details on selected topics of the PRIPARE methodology. All the modules follow a similar structure, including a set of slides to guide the explanation and a set of reference materials available for the practitioners to get further details on specific topics of their interest. Some topics will include templates and examples of use too.

4.4.1 General Knowledge

This first module aims at providing practitioners with general knowledge regarding privacy-by-design principles and concepts e.g. what privacy-by-design is, why it matters, the PbD

foundational principles, the benefits of applying a PbD methodology, etc. The goal of this material is to introduce the topic from an ICT practitioner point of view, providing an overview of related terms, and motivating and introducing the next themes.

By following this module practitioners will:

1) be aware of the privacy-by-design concept and related terms;
2) know the PRIPARE principles supporting PbD;
3) understand why PbD matters and the benefits of applying a PbD methodology to a software or system development process.

The material for this module will include:

- A set of slides to guide the explanation, including definitions of concepts, terms and the PRIPARE principles.
- Reference material for practitioners where some of the terms and principles are further discussed. PRIPARE deliverable D1.1 and PRIPARE position paper are examples of this reference material, as well as articles in the domain that provide an overview of PbD methodologies and related terms.

The set of slides for this module will be available by M9 (June 2014) and will be produced by the PRIPARE project. Some reference material will be added to the module in M6 (March 2014) i.e. PRIPARE Deliverable 1.1 and PRIPARE position paper. Reference materials produced somewhere else will be added to the module once it has been evaluated and found appropriate.

4.4.2 Specific Knowledge

The goal of this module is to introduce and describe specific topics of the PRIPARE methodology. Each topic will include a light introduction to the theme, followed by an explanation including technical details. The topics included are:

1. PRIPARE methodology: An overview.
2. Privacy requirements engineering.
3. Privacy impact assessment and risk analysis.
4. PRIPARE best practices.
5. Privacy Patterns
6. Failures in Privacy Systems
7. Privacy Design Strategies
8. Location Privacy
9. Anonymous Cash

The material for the first topic i.e. *PRIPARE methodology*, will include:

- A set of slides to guide the explanation, including the description of the steps of the PRIPARE methodology, the processes involved and the resulting artefacts.
- Reference material for practitioners where specific steps, processes or artefacts are detailed. PRIPARE deliverable D1.2 is an example of this reference material, since it will define the PRIPARE methodology in detail.

The set of slides for this first topic will be available by M15 (December 2014) and will be produced by the PRIPARE project. The PRIPARE Deliverable 1.2 will be added as reference material in M15. Other reference materials external to the project will be added to this topic once they have been evaluated and found appropriate.

The material for the *Privacy requirements engineering* topic will include:

- A set of slides, which describes the privacy context (Legal, ethical, economic and social context) that should be considered to gather privacy requirements. It will also describe how privacy principles can be translated into system functions that can be addressed by engineers.
- Reference material for practitioners covering different aspects on the privacy context and on how to translate privacy principles into requirements. PRIPARE deliverable D1.2 is an example of this reference material.

The set of slides for this topic will be available by M15 (December 2014) and will be produced by the PRIPARE project. The PRIPARE Deliverable 1.2 will be added as reference material in M15. Other reference materials external to the project will be added to this topic once they have been evaluated and found appropriate.

The material for the *Privacy impact assessment and risk analysis* topic will include:

- A set of slides describing the related terminology such as privacy risks, threats, vulnerabilities, privacy impact assessment, and risk analysis. In addition, it will describe what elements a privacy impact assessment should contain, how it relates to risk analysis and management, and how to carry out them. It will also describe procedures to deal with those risks found in case they materialise, and propose practical approaches for the choice and/or development of effective privacy controls.
- Reference material for practitioners covering privacy impact assessment and privacy risks analysis and management. PRIPARE deliverable D1.2 is an example of this reference material.
- A template useful to carry out a privacy impact assessment.
- Some examples of privacy impact assessments.

The set of slides for this topic will be available by M15 (December 2014) and will be produced by the PRIPARE project, although an early version will be available by M12. The PRIPARE deliverable 2.2 will be added in M9, the PRIPARE Deliverable 1.2 will be added as reference material in M15, and the PRIPARE deliverable D2.3 will be added in M15. A PIA template will be made available also by M9. Example of PIAs will be available through the Web portal in M15. Other reference materials external to the project will be added to this topic once they have been evaluated and found appropriate.

The material for the topic *PRIPARE Best practices,* will include:

- A set of slides describing what a best practice is in the context of a PbD methodology. In addition, it will include examples of best practices such as PIAs and privacy patterns, as well as a description on how to understand and apply them. Finally, it will introduce the PRIPARE catalogue of best practices, and will explain the guidelines to create new best practices and add them to the catalogue.
- Reference material for practitioners covering different aspects on best practices, and documents describing examples of best practices. PRIPARE deliverables D2.1, D2.2, D2.3 and D2.4 are examples of these reference materials.
- Templates for different kinds of best practices such as PIAs or privacy patterns.
- Examples of different kinds of best practices.

- A catalogue of best practices where practitioners can refer to in order to find new examples of best practices.

An early set of slides for this topic will be available by M15 (December 2014) and will be produced by the PRIPARE project. The PRIPARE deliverables D2.1, D2.2 and D2.3 will be added as reference material in M15, while PRIPARE deliverable D2.4 will be added in M21. Templates and examples will be added as they are produced by the PRIPARE project. The catalogue will be made available in M15, as planned in PRIPARE WP2. Other reference materials external to the project will be added to this topic once it has been evaluated and found appropriate.

The material for the *Privacy Patterns* topic will introduce the topic of privacy patterns, together with their possibilities and limitations. The presentation form will be a set of slides and a catalogue of privacy patterns. Furthermore, we provide references to other reading material.

The material for the topic *Failures in Privacy Systems* discusses some examples of privacy systems which failed. This material will examine common problems which are often overlooked in the design of privacy systems, which have resulted in a breach.

The material for the *Privacy Design Strategies* topic is organized in eight subtopics, namely *Minimize, Hide, Separate, Aggregate, Inform, Control, Enforce,* and *Demonstrate.* This categorization is inspired by the work of Hoepman[55].

- *Minimize*: The idea is to restrict the amount of information that is being collected.
- *Hide*: This design strategy aims to hide the data in a larger anonymity set, or alternatively, hides the correlation between different data sets.
- *Separate*: In this subtopic we examine technologies that distribute the processing of personal information to avoid the creation of personal profiles.
- *Aggregate*: This design strategy suggests that personal data is always processed at the highest possible level of aggregation and with the least possible detail. A concrete technology that is known to implement this approach is group signatures.
- *Inform*: In this subtopic we examine ways how to inform the data subject over the data it provides and its use.
- *Control*: This subtopic explains Hoepman's *Control* privacy design strategy, i.e., it examines the ways in which a data subject can control his or her data.
- *Enforce*: The design strategy *Enforce* treats ways how one can enforce privacy policies.
- *Demonstrate*: Hoepman's strategy *Demonstrate* comprises technologies how a service provider is able to prove his compliance with privacy policies and other legal requirements.

The material for the *Location Privacy* topic will examine the role of privacy in transport systems and mobile networks. This will include a discussion of C2X communication, mobile networks, the associated possibilities and risks.

Finally, the material for the last topic, *Anonymous Cash* will introduce the ideas and principles of anonymous payment systems. Furthermore, we examine some famous examples like

[55] Hoepman, Jaap-Henk. "Privacy design strategies." (2012) http://arxiv.org/pdf/1210.6621.pdf

DigiCash, *eCash* and *Bitcoins*. The material will consist of a set of slides, together with some exercises.

4.5 Students

4.5.1 General knowledge

- Privacy in ICT environments - Overviews of privacy basic concepts, its definitions and current related ethical problems and solutions.

4.5.2 Specific knowledge for CS/IT students:

- Privacy Enhancing Technologies – A set of Reading list and pointers to existing material describing privacy preserving technologies including their capabilities and limitations.

- Privacy in ICT environments – will provide slides, exercises and reading lists for several themes including:
    - Secure programming with technical descriptions of how security and privacy related techniques are considered in programming practices;
    - Introduction to the Internet of Things and the emerging privacy issues involved;
    - Privacy enhancing techniques for Web Services: Introduction to current web services, such as SOAP, WSDL, and REST and how they address privacy
    - an Introductions on building privacy and security into technology products and services and the related trade-offs. Integration of privacy protection and security into the overall engineering lifecycle of such products and services including requirements, design and testing phases;
    - Descriptions of background issues in Web security and common vulnerabilities. The relationship of those vulnerabilities to user and consumer privacy
    - Introduction to cryptography techniques with references to detailed learning material particularly in relation to privacy;
    - Comparison and relationship between security and privacy concepts;
    - Introductions and detailed discussions of anonymisation techniques;
    - Description of design patterns that support security and privacy and references to more detailed discussions.

- Database Privacy – Reading lists and pointers to existing material will be provided in order to introduce privacy preserving techniques in data mining and processing and current limitations, such as scalability. Slides, exercises and reading lists will be provided for:
    - Introduction to cryptography techniques for protection of data at rest
    - Descriptions of background issues in Web security and common vulnerabilities. The relationship of those vulnerabilities to user and consumer data privacy

- Cloud Privacy – Slides and reading list for introducing privacy and security patterns applicable to the cloud environments as well as references to detailed discussions

- Mobile Privacy – Existing resources on privacy issues in existing mobile device platforms.

- Economic Aspects – Slides and reading lists describing the concepts of trust, trustworthiness and reputation as well as related systems and models

- Privacy risks and incidents - Reading lists and pointers to existing material will be provided for PIAs and related discussions including its applicability to PbD as well as describe and discuss issues around compliance audits and review techniques. Slides, exercises and reading lists will be provided for a description of management of organisational privacy and security risks and the use of security metrics. Description of techniques to cope with privacy issues including identifying and dealing with privacy incidents and mitigating risks in the context of PbD. Overview of threat modelling techniques.

4.5.3 Specific knowledge for non-CS/IT students:

- History of technology and human rights treaties relevant to PbD – Two modules (slides exam questions and reading list) will be provided. One will cover the history of technology leading to the convergence underlying current privacy problems (ubiquity, storage, and connectivity). The second will cover the history of relevant human rights treaties and contemporary issues.

- Principles and processes of PbD – Slides, exam questions and reading list will be provided covering the regulatory view of PbD, PbD principles, PbD processes, PbD technologies, and current standard for operationalizing PbD

- Application of EU privacy law online - Slides exam questions and reading list will cover current EU regulation and the debate around privacy and PbD in particular

- Technology responses to privacy problems - Slides exam questions and reading list will explore how technology addresses privacy issues. Perspectives and limitations will be analysed through different paradigms and examples.

4.6 Policy makers, and governmental and non-governmental bodies acting for human rights protection

The following modules contain material for policy makers, and governmental and non-governmental bodies acting for human rights protection. The modules are separated under two sections, general or specific knowledge, based on the depth of knowledge the material addresses.

4.6.1 General knowledge

The mode of presentation for the general knowledge modules will be PowerPoint presentations and accompanied by selected reading material. The expected time of delivery for the modules is December 2015. The themes of the general knowledge modules are:

1. Existing legal sources
2. Basic principles
3. Data protection reform

The *Existing legal sources* module will describe the legislative initiatives that illustrate the state of the art in the EU legal order as well as the context within which they function. The material will cover:

- The Data Protection Directive
- The E-Privacy Directive
- The Data Retention Directive
- Regulation for data protection in EU institutions

The *Basic principles* module will elaborate on the content of each of the following principles and its importance for the protection of the rights of the individual in the EU. The principles addressed are:

- Consent principle
- Data minimization (proportionality)
- Data quality
- Purpose specification/limitation
- Transparency
- User's right of access/right to object
- Confidentiality and security of processing
- Obligation to notification
- Data retention
- Right to erasure

The third and final module under general knowledge for legal and policy makers is *Data protection reform* and covers:

- General Data protection Regulation
- Data protection Directive for the processing of data by law enforcement authorities
- And the major changes

The module explains the reasons that triggered the data protection reform, analyses its content and discusses the major changes that are envisaged in the two proposals.

4.6.2 Specific knowledge

This section has two parts and the mode of presentation for the modules will be PowerPoint presentations accompanied by select reading material. The expected time of delivery of *Part I* is December 2014, proceeded by *Part II* in December 2015.

4.6.2.1 Part I: Context. The concept of Privacy by Design

Part I contains the following two modules:

- **How did the concept develop?** (Context: PbD, PETs, Europrise seal, etc.)
  This module analyses how PbD developed in the EU and internationally. Of particular interest is the work of some European DPAs as well as of the EDPS that stressed the importance of the data minimization principle some time ago. The Information and Privacy Commissioner of Ontario, Canada has articulated the foundational PbD principles and progressively advanced ways to operationalize PbD. All DPAs underline that the use of PETs is instrumental to prevent undesired processing of personal data. Additionally, the European Commission has later endorsed PETs as tools to achieve data minimization without undermining the functionality of an IT system. The link between data protection laws and PETs has also been illustrated through the general obligation to security (Article 17 of the Data Protection Directive).

  Meanwhile, the European Commission, as well as the EDPS and the 29WP had started to refer explicitly to endorsement of the principle of PbD that stems from the need to build privacy into information systems. The latest expression of this trend is found in the two drafts (From section 4.4.1, see *Data protection reform*), where PbD is finally introduced as a legal principle.

- **How PbD is implemented in the draft regulation?**
  This module elaborates on how the draft regulation reinforces PbD. We are taking a broader view discussing privacy risk management and the subsequent need for data minimisation in the context of the obligations of the data controllers. Accountability, PbD, Privacy by Default, and PIA constitute expression of technical and organisational measures that the controller has to take in order to perform efficient privacy risk management. PbD, which is closely interconnected with users' empowerment, is also examined from the viewpoint of the data subject.

4.6.2.2 Part II: How legal principles affect the design process

Part II is made up of the following two modules and set of examples:

- **Privacy risk management:** *Data governance and PIA/privacy risk management methodologies.*
  This module discusses PbD within the general context of data governance. We examine certain risk management (e.g. PIA) and general data governance techniques (e.g. GRC) in order to conclude that PbD and accountability are crucial to achieve efficient data governance in organisation, even if the first one performs pure risk management, whereas the second one is a more general data governance technique.

- **How do legal principles affect policy making?**
  In this module privacy is perceived as a means to effective policy making. In the Commission Impact Assessment Guidelines (2009), privacy is a requirement that should be taken into account in the EU policymaking process. However, this is not always the case. Using a case study we propose a methodology that performs a 'privacy impact assessment' to the process of policy making.

- **Examples:** *Privacy by design in the field of cloud computing and biometric verification in border control.*

For each example the following structure is followed: i. Description of the status quo: What is the situation in cloud computing/biometric verification in border control? ii. What are the privacy risks posed to the rights of the individual? iii. Legal input. (EDPS, DPAs, 29WP opinions etc.) iv. How the application of PbD can ensure privacy and data protection? Compliance with the principle of data minimisation is enhanced with the use of PETs (e.g. cryptography).

5 Conclusions

Information and education are the prerequisites for the acceptance of any regulation and innovation and as such play an essential role in the successful adoption of Privacy by Design amongst its many stakeholders.

The work in task one of work package four, described in this deliverable, has concentrated on the identification of PbD stakeholders, their informational and educational needs, and the most effective manner to address these needs. This work has resulted in designing a clear road map for the development of PbD information and educational resources. This road map, described in section 4, identifies the *themes* that must be addressed for each type of stakeholder and the educational/informational *modules* that need to be developed in order to present to the themes. The remaining tasks of work package four will task with the implementation of the road map through the design and realisation of each module.

The discussions around stakeholders identification has allowed us to define two levels of needs; one that addresses stakeholders *awareness* about the objectives and role of PbD and a second one that addresses the *actions* that each stakeholder may undertake within the PbD framework; these two levels are respectively addressed by *general knowledge* modules and *specific* knowledge modules.

Our research shows that while privacy within digital environments is increasingly recognised as an issue that must be addressed at several levels and by a variety of stakeholders, the informational and educational resources available remain sparse and often concentrate on specific technologies, specific interpretation of what privacy may be, and specific regulations. As a result, even those stakeholders who are aware of the privacy problem - and who may want to gather a better understanding of the issues at stake and the actions they may undertake to protect privacy - are faced with the difficult task of navigating disparate and sometime contradictory information. On the contrary, the information and education material we propose, although organised in a modular structure, which allows possible re-use across stakeholders, is organised so to address in an organic manner all the *themes* necessary to inform and educate stakeholders. This ensures that each need/theme is addressed by at least one module. When multiple perspectives existed for the same theme (e.g. an example based approach versus a theoretical based one) we propose multiple modules covering the same theme.

We believe that the modules we have identified (and that we will implement in the rest of the project) form the basis of a collection that may be further develop in the future.

According to the DoW, the next steps for the development of the educational material will include:

- Development, by month 15, of the Initial Educational Material including the first set of General Public Education Material and Practitioner Training Material
- Development, by month 24, of the Full Educational Material including a revision of the initial material, the Education Material for ICT students, and the Information and

Reference Material for policy makers, and governmental and non-governmental bodies acting for human rights protection

6 Appendix 1 – University Programs and Courses in Privacy

(Courses highlighted are those offers by Pripare partners)

6.1 Programs in Privacy for CS/ICT student (both G and U)

- MSIT in Privacy Engineering[56] - Carnegie Mellon (1 year program, G)
  - Core courses: - Information Security and Privacy - Privacy Policy, Law, and Technology - Foundations of Privacy - Law of Computer Technology - Usable Privacy and Security - Engineering Privacy in Software - Management of Software Development for Technology Executives
  - "*The Master of Science in Information Technology Privacy Engineering degree is a one-year graduate program for computer scientists and engineers who wish to pursue careers as privacy engineers or technical privacy managers. Designed in close collaboration with industry and government, this program is intended for students who aspire to play a critical role in building privacy into products, services, and processes.*"
- Security and Privacy Major[57] – EIT ICT Labs Master School (2 year program, G)
  - Information Security and Privacy specialization courses: Information Security and Privacy – Privacy Enhancing Technologies – Formal Methods in Information Security and Privacy – Practical Aspects of Information Security - Seminar on Selected Topics in Information Security and Privacy
  - "*The Information Security and Privacy specialization connects provably secure and privacy-preserving concepts with practically deployable applications. This area offers many possible directions for the students such as Android Security, Web Security, or Synthesis of Distributed Applications, to name a few. Working on these concrete domains, the student learns how to use complex cryptographic primitives as well as information flow analyses in order to guarantee privacy of software systems.*"
- Security and Privacy[58] – UMass Amherst (4 year program, UG)
  - "*We are constantly increasing our reliance on computers for managing information from tasks both great and small. In scenarios ranging from our personal lives to our nation's critical infrastructure, the security and privacy of information is a fundamental challenge in computer science.*"
- Mastère Informatique et Libertés – Institut Supérieur d'Electronique de Paris[59] (1 year program, G)
  - "*Pionnier en ce domaine, l'ISEP a créé la première formation diplômante destinée à former ces « Experts de la protection des données personnelles » : le Mastère spécialisé en Management et Protection des données à caractère personnelles , ou « Mastère Informatique et Libertés ».*"

6.2 Courses in Privacy for CS/ICT student (both G and U)

- Advanced Security and Privacy[60] - Indiana University Bloomington (1 semester, UG)
  - Recommended material:
    - "A Taxonomy of Privacy"[61] Daniel J. Solove, GWU Law School Public Law Research Paper No. 129 University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006.
    - Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management[62] — A Consolidated Proposal for Terminology, Pfitzmann, Hansen, TU Dresden

[56] http://privacy.cs.cmu.edu/
[57] http://www.masterschool.eitictlabs.eu/programme/majors/sap/
[58] https://www.cs.umass.edu/ugrad-education/information-assurance
[59] http://www.informatique-et-libertes-formation.fr/mast%C3%A8re-sp%C3%A9cialis%C3%A9-informatique-et-libert%C3%A9s/
[60] http://www.cs.indiana.edu/%7Ekapadia/courses/I400/index.html
[61] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622
[62] http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf

        - Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, Robert Gellman, World Privacy Forum (2009).[63]
        - Low-Cost Traffic Analysis of Tor S.J. Murdoch, G.Danezis, IEEE Security and Privacy (Oakland) 2005[64]
        - Full resource list[65]
    - "*This course will cover several security concepts through the lens of privacy. Topics include peer-to-peer and anonymizing networks, personal data in the cloud, usable design for control over personal information, social networking, location and activity sharing, privacy of personal health records, and cryptographic techniques for enhancing privacy. We will also discuss legal issues related to network communication, electronic publishing of photos and videos, and data in the cloud*"
- Information Security and Privacy[66] - Carnegie Mellon (1 semester, G)
    - Recommended material:
        - *E-commerce: Business, Technology, Society*[67], 3rd edition, Kenneth C. Laudon and Carol Guercio Traver, Addison Wesley, 2007
        - *Web Security, Privacy and Commerce*[68], 2nd edition, Simson Garfinkel, O'Reilly, 2002.
    - *"The objective of this course is to introduce students to Web Security and Privacy technologies as well as to related business, legal, policy and usability issues."*
- Usable Privacy and Security[69] - Carnegie Mellon (1 semester, G)
    - Recommended material:
        - *Security and Usability: Designing Secure Systems that People Can Use*[70], edited by Lorrie Cranor and Simson Garfinkel
        - *Research Methods in Human-Computer Interaction*[71]. Lazar J, Feng J, Hochheiser H.
        - *I Didn't Buy it for Myself': Privacy and Ecommerce Personalization*[72]. Lorrie Faith Cranor, In Clare-Marie Karat, Jan O. Blom, and John, Karat, eds. *Designing Personalized User Experiences in eCommerce*[73]. Kluwer Academic Publishers, 2004.
        - *The Role of Privacy Enhancing Technologies*[74]. Lorrie Faith Cranor. In *Considering Consumer Privacy: A Resource for Policymakers and Practitioners*. Center for Democracy and Technology, edited by Paula J. Bruening, March 2003.
        - *End-User Privacy in Human-Computer Interaction*[75], Giovanni Iachello Jason Hong (2007), Foundations and Trends in Human-Computer Interaction: Vol. 1: No 1, pp 1-137.
        - *Privacy in the United States: Some Implications for Design*[76], Christena Nippert-Eng, International Journal of Design, 1(2), 1-10.
        - *Privacy Guidelines for Developing Software Products and Services*[77], Microsoft, 2007.
        - *Full resource list*[78]
    - "*There is growing recognition that technology alone will not provide all of the solutions to security and privacy problems. Human factors play an important role in these areas, and it is important for security and privacy experts to have an understanding of how people will interact with the systems they develop. This course is designed to introduce students to a variety of*

[63] http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf
[64] http://www.cl.cam.ac.uk/users/sjm217/papers/oakland05torta.pdf
[65] http://www.cs.indiana.edu/%7Ekapadia/courses/I400/resources.html
[66] http://www.normsadeh.com/isp-course-objective
[67] http://www.amazon.com/exec/obidos/tg/detail/-/0321269373/qid=1095275165/sr=8-1/ref=pd_csp_1/104-3723431-7413543?v=glance&s=books&n=507846
[68] http://www.amazon.com/exec/obidos/tg/detail/-/0596000456/qid=1095275249/sr=1-1/ref=sr_1_1/104-3723431-7413543?v=glance&s=books
[69] http://cups.cs.cmu.edu/courses/ups-fa11/#texts
[70] http://www.oreilly.com/catalog/securityusability/index.html
[71] http://www.wiley.com/WileyCDA/WileyTitle/productCd-EHEP001660.html
[72] http://lorrie.cranor.org/pubs/personalization-privacy.pdf
[73] http://www.wkap.nl/prod/b/1-4020-2147-X
[74] http://www.cdt.org/privacy/ccp/roleoftechnology1.shtml
[75] http://www.nowpublishers.com/product.aspx?product=HCI&doi=1100000004
[76] http://www.ijdesign.org/ojs/index.php/IJDesign/article/view/67
[77] http://www.microsoft.com/downloads/details.aspx?FamilyID=c48cf80f-6e87-48f5-83ec-a18d1ad2fc1f&displaylang=en
[78] http://cups.cs.cmu.edu/courses/ups-fa11/readings.html

usability and user interface problems related to privacy and security and to give them experience in designing studies aimed at helping to evaluate usability issues in security and privacy systems. The course is suitable both for students interested in privacy and security who would like to learn more about usability, as well as for students interested in usability who would like to learn more about security and privacy."

- Foundations of Privacy[79] - Carnegie Mellon (1 semester, G)
  - Recommended material:
    - Reading list and course slides[80]
  - "*Privacy is a significant concern in modern society. Individuals share personal information with many different organizations - healthcare, financial and educational institutions, the census bureau, Web services providers and online social networks - often in electronic form. Privacy violations occur when such personal information is inappropriately collected, shared or used. We will study privacy in a few settings where rigorous definitions and enforcement mechanisms are being developed - statistical disclosure limitation (as may be used by the census bureau in releasing statistics), semantics and logical specification of privacy policies that constrain information flow and use (e.g., by privacy regulations such as the HIPAA Privacy Rule and the Gramm-Leach-Bliley Act), principled audit and accountability mechanisms for enforcing privacy policies, anonymous communication protocols - and other settings in which privacy concerns have prompted much research, such as in social networks, location privacy and Web privacy (in particular, online tracking & targeted advertising).*"
- Engineering Privacy in Software[81] - Carnegie Mellon (1 semester, G)
  - Recommended material
    - Requirements Engineering: From System Goals to UML Models to Software Specifications. Axel van Lamsweerde (2009), New Jersey: John Wiley & Sons, Inc.
  - "*This graduate-level course covers the methods and tools needed to design systems for privacy with a specific focus on the requriements, design and testing stages of the software development lifecycle."*
- Privacy Enhancing Technologies: From Theory to Practice[82] – University of Maryland (1 semester, UG)
  - "*The general theme of this course is to explore potential techniques for building new platforms, services, and tools that protect users' privacy. In particular, we emphasize the technical and economic viability, as well as the usability of these privacy technologies. We will study promising component technologies ranging from advances in secure systems research (e.g., trusted computing, virtualization), to theoretic tools like differential privacy and cryptography*."
- Local Data and User Privacy[83] – University of Maryland (1 semester, UG)
  - "*Local data refers to information that is available without accessing a wide-area network. Local data can be gathered by environmental sensors or generated by users, and is usually 'tagged' with context such as location and time. As part of this course, we will concentrate on systems and protocols for small form-factor computing devices, e.g. smart phones and tablets, that enable spontaneous and opportunistic gathering and dissemination of local data. Topics will include overall system design, data delivery models, principals and naming, content-based routing, and application areas*."
- Trust, Security and Privacy Management - University of Kent (PG)
  - *"This module investigates the whole process of security management. A holistic view of security management is taken, starting with risk management and the formulation of security policies. Technical subjects include a description of the various security models, and showing how authorisation policies can be automatically enforced. The legal and privacy issues associated with information management are also addressed, as are the usability issues of security technologies. Finally, the module concludes by investigating how security has already been inbuilt into some existing applications, and how security issues will effect the uptake of ubiquitous computing systems."*
- Ethics & e-Privacy - Waterford Institute of Technology (PG)
  - *The module in MSc in Information Systems Processes programme. "The rate of ICT development has outpaced society's ability to regulate responsible usage of such technologies. Technology has a profound effect on many aspects of work, life and society and this implies significant*

[79] https://www.ece.cmu.edu/~ece734/
[80] https://www.ece.cmu.edu/~ece734/schedule.htm
[81] http://www.cs.cmu.edu/~breaux/teaching-08605sp14.html
[82] http://www.cs.umd.edu/~elaine/teaching/privacy-f12/
[83] http://www.cs.umd.edu/class/spring2012/cmsc818c/

responsibility for the purveyor of such systems – the ICT professional. This module will provide students with a critical awareness of, and skills to cope with, many of the most ethically charged ICT issues in modern society including e-Privacy."

- Security, Privacy, and Trust[84] – American University of Paris (1 semester, UG)
  - Recommended material
    - Daniel Solove, 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy, San Diego Law Review, Vol. 44, 2007.
    - Daniel Solove, A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006.
    - Understanding privacy. Harvard university press, by Daniel Solove, 2008
  - *"The course provides an understanding on the need for security, privacy and trust in ICT. Legal and ethical aspects will be covered. Technology for security, privacy and trust will be presented at a functional level."*
- Privacy in a Networked World[85] - Stevens Institute of Technology (Online Syllabus[86])(1 semester, G)
  - Recommended material:
    - S. Garfinkel, *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly, 2001.
    - R. O'Harrow, *No Place to Hide*, Free Press, 2006.
  - Learning goals or "Course Outcomes"[87]
- A Study of Perturbation Techniques for Data Privacy[88] – Stanford University (Online Syllabus[89]) (1 semester, UG)
  - Recommended material:
    - See reading list in syllabus
  - *"The digital age has enabled widespread access to and collection of data. While there are several advantages to ubiquitous access to data, there is also the potential for breaching the privacy of individuals.*
    In a statistical database, personal information about n individuals is typically stored (n is usually very large). A statistical database system gives users the ability to obtain aggregate statistical information (like medians, averages, counts) and yet also preserve the privacy of individuals. Typical applications include medical, financial, and census data.
    The course will study techniques for simultaneously enabling access to aggregate data and preserving privacy. Data perturbation is a classical technique for solving this problem. There are two flavors of data perturbation. In one version, the data are perturbed once, and the perturbed values are published. In the second version, the data are held secret; the database algorithm computes the true response to queries, and adds noise to the answer, reporting only the noisy answer. Both versions of the problem have a rich literature."
- Security and Privacy in Mobile Systems – University of Ulm (1 semester, G)
  - *"Participants know the major threats to security and privacy in mobile systems and know how to select and design suitable security mechanisms to protect from them. They are capable of analyzing the security of mobile communication systems and wireless networks on all layers. They can identify and analyze weaknesses and understand the presented attacks. Furthermore, students can propose and discuss possible security solutions to protect systems appropriately. Beyond, they understand the role and importance of location privacy and data protection in mobile systems and are familiar with the most important privacy enhancing technologies."*
  - *"The course provides a deepened discussion of security and privacy for mobile systems. After an introduction into the specifics of mobile systems, the course continues with discussing specific security and privacy requirements. The lecture is composed of two main blocks. The first block introduces and discusses security issues and security mechanisms of established mobile communication systems such as WLAN, cellular networks, Bluetooth, or RFID. In the second part, the lecture provides an introduction to current research topics related to mobile security and privacy, e.g., in the areas of mobile ad-hoc networks or VANETs."*
- Sensitive Information in a Wired World[90] – Yale University (1 Semester, UG/G)
  - Reading Material under 'Assignments' section on course website

[84] http://www.aup.edu/academics/course-catalog/cs2055/spring-2014
[85] http://www.stevens.edu/compsci/graduate/masters/courses/viewer.php?course=CS578&type=syl
[86] http://www.stevens.edu/compsci/graduate/masters/courses/viewer.php?course=CS578&type=syl
[87] http://www.stevens.edu/compsci/graduate/masters/courses/viewer.php?course=CS578&type=o
[88] http://theory.stanford.edu/~nmishra/cs369-2004.html
[89] http://theory.stanford.edu/~nmishra/cs369-2004.html
[90] http://zoo.cs.yale.edu/classes/cs457/fall13/

- "*Increasing use of computers and networks in business, government, recreation, and almost all aspects of daily life has led to a proliferation of online sensitive data. Sensitive data are those that, if used improperly, can harm the data subjects, data owners, data users, or other interested parties. As a result, concern about the ownership, control, privacy, and accuracy of these data has become a top priority. This course focuses on both the technical challenges of handling sensitive data and the policy and legal issues facing data subjects, data owners, and data users.*"

- Advanced Topics in Computer Science: Privacy Technologies[91] – Princeton University (Annotated Syllabus[92]) (1 semester, G)
  - Recommended Material
    - Dan Solove. *Why Privacy Matters Even if You Have 'Nothing to Hide'*[93] (Chronicle)
    - David Brin. *The Transparent Society*[94] (WIRED, circa 1996, later expanded into a book)
    - More in the privacy section of the reading list
  - "*Numerous privacy-enhancing technologies have been developed in the last few decades, often utilizing powerful math and algorithms. The results have been mixed — some have been successful while others have seen little adoption despite much hype and promise. In this course we will study privacy technologies, their uses and limitations, the reasons for their success and failure, and think critically about their place in society. More broadly, we will also try and understand the implications of ubiquitous data collection, aggregation and profiling.*
    On the technical end we will study topics like cryptography, differential privacy and anonymity (including Tor and Bitcoin). On the other hand we will see what scholars from the fields of human-computer interaction, law, economics, etc., as well as journalists and even sci-fi authors have to say about privacy technologies. Some of these papers include discussions of topics as diverse as 19th century railroads and piracy (the nautical kind!).
    To accommodate students with varying levels of technical background, evaluation will be project-focused. You can choose a programming-based or essay/paper-based project."

6.3 Socio-Ethical and Legal courses

- Information Ethics - Course WordPress site[95] - Indiana University Bloomington (Online syllabus[96]) (1 semester, UG)
  - Recommended material:
    - *How Much Should People Worry About the Loss of Online Privacy?*[97] The Wall Street Journal (11/15/2011)
    - *"I've Got Nothing to Hide, and Other Misunderstandings of Privacy"*[98], Daniel J. Solove, George Washington University Law School, San Diego Law Review, Vol. 44, 2007
    - *"The Perfect Mark: How a Massachusetts psychotherapist fell for a Nigerian e-mail scam"*[99], Mitchell Zuckoff, New Yorker (2006)
    -
  - "*This course explores the ethical and professionalization issues that arise in the context of designing and using information technologies. We will study the major ethical theories and frameworks that have shaped the field of information ethics and use them to address topics relevant to the informatics profession, including privacy, intellectual property, cybercrime, games, social justice, gender equity.*"
- Privacy Policy, Law, and Technology[100] - Carnegie Mellon (1 semester G)
  - Recommended material:
    - In Privacy Handbook for IT Professionals, T. Breaux, 2013
    - Privacy as Part of the App Decision-Making Process[101]. P.G. Kelley, L.F. Cranor, and N. Sadeh. CHI 2013.

[91] http://randomwalker.info/teaching/fall-2012-privacy-technologies/
[92] http://petsymposium.org/2013/papers/narayanan-teaching.pdf
[93] http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/
[94] http://www.wired.com/wired/archive/4.12/fftransparent_pr.html
[95] http://homes.soic.indiana.edu/nensmeng/courses/i453ethics.html
[96] http://homes.soic.indiana.edu/nensmeng/files/i453-syllabus.pdf
[97] http://online.wsj.com/news/articles/SB10001424052970204190704577024262567105738
[98] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565
[99] http://www.newyorker.com/archive/2006/05/15/060515fa_fact
[100] http://cups.cs.cmu.edu/courses/pplt-fa13/

- Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents[102] Rubinstein, Ira and Good, Nathan, (August 11, 2012). Berkeley Technology Law Journal, Forthcoming.
- Misplaced Confidences: Privacy and the Control Paradox[103]. L. Brandimarte, A. Acquisti, G. Loewenstein. Social Psychological and Personality Science May 2013 vol. 4 no. 3 340-347.
- Fair Information Practices: A Basic History[104]. Robert Gellman Version 1.92, June 24, 2013.
- A Cross-Cultural Framework for Protecting User Privacy in Online Social Media[105]. B. Ur and Y. Wang. In WWW Workshop on Privacy and Security in Online Social Media (PSOSM13), Rio de Janeiro, Brazil, 2013.
- The Cost of Reading Privacy Policies[106]. A. McDonald and L. Cranor. *I/S: A Journal of Law and Policy for the Information Society*. 2008.
- Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice[107]. L.F. Cranor. Journal of Telecommunications and High Technology Law, Vol. 10, No. 2, 2012.
- Privacy Self-Management and the Consent Dilemma[108], Solove, Daniel J., 126 Harvard Law Review 1880 (2013).
- Privacy on the go: recommendations for the mobile ecosystem[109], K. Harris, California Department of Justice, January 2013.
- Privacy Guidelines for Developing Software Products and Services[110], Microsoft, 2007.
- Engineering Privacy[111]. Sarah Spiekermann and Lorrie Faith Cranor. *IEEE Transactions on Software Engineering* Vol. 35, No. 1, January/February, 2009, pp. 67-82.

o *"This course focuses on policy issues related to privacy from the perspectives of governments, organizations, and individuals. We will begin with a historical and philosophical study of privacy and then explore recent public policy issues. We will examine the privacy protections provided by laws and regulations, as well as the way technology can be used to protect privacy. We will emphasize technology-related privacy concerns and mitigation, for example: social networks, smartphones, behavioural advertising (and tools to prevent targeted advertising and tracking), anonymous communication systems, big data, and drones."*

- Privacy in the Digital Age[112] - Carnegie Mellon (1 semester, G)
  - Recommended material
    - Technology and Privacy: The New Landscape, Agre and Rotenberg
    - Database Nation, Garfinkel
    - Ben Franklin's Website, Robert Ellis Smith
    - The Digital Persona, Daniel Solove
  - *"Privacy is a complex and multi-faceted concept. This course combines technical, economic, legal, and policy perspectives to present a holistic view of its role and value in the digital age."*
- Privacy Versus In-Your-Face Big Government[113] – University of Maryland (Online Syllabus[114]) (1 semester course, UG)
  - *"The essence of this course is control of information, whether by individuals (in defense against an out of control government), by government (in the interests of its effectiveness on our behalf) or by the commercial sector (as intellectual property in the interests of a robust economy.) We will*

[101] https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab13003.pdf
[102] http://ssrn.com/abstract=2128146
[103] http://www.heinz.cmu.edu/%7Eacquisti/papers/acquisti-SPPS.pdf
[104] http://bobgellman.com/rg-docs/rg-FIPShistory.pdf
[105] http://precog.iiitd.edu.in/events/psosm2013/ur_wang_psosm13_culturalframework.pdf
[106] http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf
[107] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2184059
[108] http://ssrn.com/abstract=2171018
[109] http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf
[110] http://www.microsoft.com/downloads/details.aspx?FamilyID=c48cf80f-6e87-48f5-83ec-a18d1ad2fc1f&displaylang=en
[111] http://ssrn.com/abstract=1085333
[112] http://master.econ.uni-freiburg.de/students/courses/1prof._acquisti_syllabus.pdf
[113] http://doubletap.cs.umd.edu/purtilo/239R/
[114] http://doubletap.cs.umd.edu/purtilo/239R/2014/syllabus.html

tour the competing technologies and specifically evaluate their interplay with both enumerated and natural rights. We will study the role of computers in this balancing act and try to understand the mechanisms underlying the privacy dynamic."

- Privacy and Technology[115] – Harvard University (Online Syllabus[116])(1 semester, UG)
  - *"What is privacy, and how is it affected by recent developments in technology? This course critically examines popular concepts of privacy and uses a rigorous analysis of technologies to understand the policy and ethical issues at play. Case studies: database anonymity, research ethics, wiretapping, surveillance, and others. Course relies on some technical material, but is open and accessible to all students, especially those with interest in economics, engineering, political science, computer science, sociology, biology, law, government, and philosophy."*
- Social and Ethical Issues in Computing[117] – University of New Mexico (Downloadable Syllabus[118])(1 semester, UG)
  - Recommended material:
    - A Gift of Fire, Sara Basse, 2nd edition, Prentice Hall, 2003
    - Full supplementary reading list[119]
  - *"Overview of philosophical ethics, privacy and databases, intellectual property, computer security, computer crime, safety and reliability, professional responsibility and codes, electronic communities and the Internet, and social impact of computers. Students make oral presentations and produce written reports. Open only to students admitted into the bachelor's degree program."*
- Human Rights and Digital Technology[120] – The American University of Paris (Online Syllabus)
  - *"When we speak of digital technology, our focus is often prohibitively narrow. Taking our cues from scientific research models, we examine the parts, rather than the whole, inadvertently isolating software from hardware, the technological frameworks from their actual use, or the costs of the digital revolution from the benefits. This course joins two seemingly disparate disciplines – law and science – in an attempt to understand more fully the dense, multidimensional nature of the digital revolution and how we are going to live with it. While it is somewhat risky to predict the outcome of a revolution, we find the application of a human rights framework extremely useful in highlighting many of the connected aspects of this technological transition. We have designed our course as an interdisciplinary primer, a guide to examining the critical issues that shape our use of digital technology; by elaborating specific case studies, we ground our general arguments in lived experiences across diverse geographic contexts. The focus of this semester course will be on privacy"*
- Special Topics in Technology Studies: Digital Media and Privacy[121] – New York University (1 semester, UG)
  - Recommended material:
    - Nissenbaum, H. (2009) Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford: Stanford University Press)
    - Regan, P. (1995) Legislating Privacy: Technology, Social Values, and Public Policy
  - "*Digital technologies have dramatically altered the shape of communications and information flows in societies, enabling massive transformations in the capacity to monitor behaviour, to amass and analyze personal information, and to distribute, publish, communicate and disseminate it. As a result, some would claim, they have radically and irrevocably diminished privacy and provoked social anxiety, inspiring new laws and policies, widespread advocacy efforts, and technical responses aimed at mitigating and resisting their impacts.*
    All of this falls within the scope of the seminar, which undertakes a multi-faceted, multi-disciplinary examination of the relationship between privacy and technology, extending back to applications of old technologies such as photography and wiretaps but focusing on technical innovations in digital media and information sciences from databases and video surveillance to biometrics, the Web, social networks, and more. Because it is hardly ever possible to draw a straight line between technology and social implication, our study will be broadly encompassing, including in its scope the people, practices, institutions, and vested interests that have supported

[115] http://isites.harvard.edu/course/colgsas-9751
[116] http://isites.harvard.edu/icb/icb.do?keyword=k88447&pageid=icb.page513858
[117] http://cs.unm.edu/~pgk/293f13/
[118] http://www.cs.unm.edu/~luger/CS293Syll.doc
[119] http://www.cs.unm.edu/~luger/ethics_cs293.html
[120] http://ac.aup.fr/~croda/lw5091/
[121] http://www.nyu.edu/projects/nissenbaum/Special_Topics_In_Technology_Studies.html

the application of technologies to monitor people, store information about them, and predict, even shape their actions. That is to say, we will be studying the relationship between privacy and key socio-technical systems."

- Societal Impact of Information Technologies[122] – Stevens Institute of Technology (1 semester, UG)
  - *"Students explore tradeoffs posed by modern information technologies such as the Internet, mining of personal data, web tracking, and surveillance systems. Also covered are major debates about how IT technologies should be harnessed to serve the greater good, such as: Internet governance, privacy vs. openness, and laws regarding intellectual property. Students will learn how actions undertaken in their daily lives as IT professionals may have broad consequences, both planned and unplanned. Students will learn how to identify and analyze these consequences and who may be affected by them. Student must be a senior computer science or cybersecurity major."*

6.4 Courses on privacy for non-CS students

- Privacy in an Age of Information Technology[123] – New York University (1 semester, UG)
  - Recommended material:
    - Priscilla Regan. Legislating Privacy: Technology, Social Values, and Public Policy (Chapel Hill: The University of North Carolina Press, 1995)
    - Judith Wagner DeCew. In Pursuit of Privacy: Law, Ethics, and the Rise of Technology (Ithaca: Cornell University Press, 1997)
  - "*The seminar comprises three parts. In the first, it examines real cases where record-keeping practices and surveillance have become controversial. Through these cases, we learn about the capabilities of contemporary technologies of information and ask probe various issues. These cases include anonymity on the Internet, privacy of medical and genetic information, and the comprehensive network of government and privately held databases. In the second part of the seminar, we move beyond analysis of actual practice to appreciate conceptual, legal and ethical foundations. We examine leading philosophical and legal theories of privacy asking such questions as: What is privacy? Why do we value it? Do we have a legal right to it? Do we have a moral right to it?*
    In the final part, we extend our vision to the broader social context and examine the relationship between privacy and other values associated with a free and democratic society. Our discussion will also cover practical aspects of contemporary privacy policy."

6.5 Courses on security that also cover privacy

- Systems & Protocol Security & Information Assurance[124] - Indiana University Bloomington (1 semester, G/UG)
  - Recommended material:
    - Department of Defense Trusted Computer System Evaluation Criteria[125], DoD 5200.28-STD. December 1985.
    - The Protection of Information in Computer Systems[126], Jerome H. Saltzer and Michael D. Schroeder, Massachusetts Institute of Technology Cambridge, Mass. USA 1975
    - "I've Got Nothing to Hide, and Other Misunderstandings of Privacy"[127] Daniel J. Solove, George Washington University Law School, San Diego Law Review, Vol. 44, 2007.
    - "A Taxonomy of Privacy"[128], Daniel J. Solove, GWU Law School Public Law Research Paper No. 129 University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006.
    - Intercepting Mobile Communications: The Insecurity of 802.11[129], Nikita Borisov, Ian Goldberg, David Wagner, MOBICOM, July 2001.

[122] http://m.stevens.edu/academics/course_desc.php?course_id=3105&prog_id=45
[123] http://www.nyu.edu/projects/nissenbaum/courses_privacy.html
[124] http://www.cs.indiana.edu/~kapadia/courses/I433-533-Spring-11/index.html
[125] http://csrc.nist.gov/publications/history/dod85.pdf
[126] http://www.acsac.org/secshelf/papers/protection_information.pdf
[127] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565
[128] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622

        - *Full resource list*[130]
    - *"This course will cover the design and analysis of secure systems. It will combine theoretical understanding with hands-on experience in adopting individual security protocols and technologies to develop a functioning whole. The course will be structured around a semester-long group project to build a secure location sharing system much like Google Latitude. Students will learn to apply techniques related to authentication, access control, database security, network security, privacy, usability, and so on."*
- Enterprise Security and Information Assurance[131] – Stevens Institute of Technology (Online Syllabus[132]) (1 semester, G)
- Security in IT Systems – University of Ulm (1 semester, UG)
    - *German language course that provides a broad introduction to IT security and privacy, including about 4 hours of lecture on privacy.*
- Computer Security and Privacy[133] – Stanford University (1 semester, UG)
    - Recommended material:
        - Privacy on the Line: The Politics of Wiretapping and Encryption by Whitfield Diffie and Susan Landau
        - The Right to Privacy by Ellen Alderman and Caroline Kennedy
    - "*The course will be based on a series of readings, with discussion of current issues in computer security. Part of the course will be devoted to current events in computer security, drawn from comp. risks and security advisories that are issued during the term. We will cover some basic issues in cryptography, including a brief summary of relevant mathematics, and computer system risks and vulnerabilities. Part of the course will also be devoted to legal and policy issues, such as censorship, rights of ownership, and rights to privacy. In this connection, we will look a computer security policy on Campus and discuss the Stanford Computer Use Policy. Each student will be required to write a term paper or present an oral report in class.*"

6.6 Certification Programs for Practitioners

1. Certified Information Privacy Professional/Information Technology (CIPP/IT)[134] - International Association of Privacy Professionals (IAPP)
    - Description: "*The CIPP/IT demonstrates understanding of privacy and data protection practices in the development, engineering, deployment and auditing of IT products and services.*"
    - Intended audience: Professionals who are responsible for the development, engineering, deployment and/or auditing of IT products and services.
    - Subject matter areas:
        - Industry-standard guidelines for the collection, use and onward transfer of sensitive personal information
        - Privacy considerations for mapping, storing and retaining sensitive personal information
        - Privacy requirements for the installation and removal of software
        - Established methods for end-user notification and choice through IT system and product interfaces
        - System controls for identity and access management (IAM)
        - Privacy-enabling technologies (PETs)
        - Network and system hardware protection
2. Certified Information Privacy Manager (CIPM)[135] - International Association of Privacy Professionals (IAPP)

[129] http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf
[130] http://www.cs.indiana.edu/~kapadia/courses/I433-533-Spring-11/resources.html
[131] http://www.stevens.edu/compsci/graduate/masters/courses/viewer.php?course=CS594&type=syl
[132] http://www.stevens.edu/academic_files/courses/syllabus/CS594syl.pdf
[133] http://theory.stanford.edu/people/jcm/cs099j/index.html
[134] https://www.privacyassociation.org/certification/cipp_certification_programs/cipp_it
[135] https://www.privacyassociation.org/certification/cipm_certification_program

- Description: "*Achieving the CIPM designation shows that you possess a strong knowledge of privacy program governance and the skills to establish, maintain and manage a privacy program across all stages of its operational life cycle. The CIPM complements the CIPP designation by demonstrating that in addition to understanding laws and regulations around privacy, you also understand how to operationalize privacy in your organization through process and technology.*"
- Intended audience: Managers such as Chief Privacy Officers (CPO), Corporate Privacy Managers, or Risk Managers who are responsible for privacy at any level of their organization.
- Subject matter areas:
  - Creating a company vision
  - Structuring the privacy team
  - Developing and implementing a privacy program framework
  - Communicating to stakeholders
  - Performance measurement
  - The privacy program operational life cycle

3. Certificate in Data Protection[136] – The Chartered Institute for IT (BCS)
   - Description: "*The Certificate in Data Protection is designed for those with some data protection responsibilities in an organisation or who, for other reasons, wish to achieve and demonstrate a broad understanding of the law and its practical application. Developed to provide candidates with an industry recognised certification that incorporates the latest changes and updates outlined in the Data Protection Act of 1998.*"
   - Intended audience: Those who have, or wish to have, some responsibility for data protection within an organisation.
   - Subject matter areas:
     - Context: Privacy and history
     - The Law: Data Protection Act, Privacy and Electronic Communications (EC Directive) Regulations 2003, Associated legislation
     - Application: How to comply with the Act, Addressing scenarios in specific areas, Data processing topics.
4. Certified Privacy Lead Assessor[137] – Data Security Council of India (DSCI)
   - Description: "*To equip the potential assessors with necessary knowledge and tools to assess organizations privacy implementations in accordance with DSCI Assessment Framework for Privacy (DAF-P)© and DSCI Privacy Framework (DPF©).*"
   - Intended audience: Assessors, personnel or consultants who are involved in the assessment of organizations according to DSCI.
   - Subject matter areas:
     - Visibility of personal information
     - Privacy organization and relationship
     - Privacy policy and processes
     - Regulatory compliance intelligence
     - Privacy contract management
     - Privacy monitoring and incident management
     - Information Usage and Access
     - Privacy Awareness and Training
     - Personal Information Security

[136] http://certifications.bcs.org/content/ConTab/8
[137] http://www.dsci.in/taxonomypage/778

5. Certification programs in the healthcare domain:
    - HealthCare Information Security and Privacy Practitioner[138] (HCISPP): Aimed at providing knowledge and experience in security and privacy controls for personal health information.
    - Certified in Healthcare Privacy and Security[139] (CHPS®): Aimed at providing competence in designing, implementing, and administering comprehensive privacy and security protection programs in all types of healthcare organizations.

[138] https://www.isc2.org/HCISPP/Default.aspx
[139] http://www.ahima.org/certification/chps

7 Appendix 2 Complete Modules Tables

General Public				
Subject	Module	Mode of presentation	Content	Contributing partner
Dangers of privacy violations and privacy rights	Smart use of smart devices	short fiction film	Dangers of privacy violations during the use of smart devices	AUP
	A Day in the Life of Max	Infograph	Typical privacy violations	AUP
	The PbD game	board game for children	Typical privacy violations	AUP
	Do you feel observed?	printed brochure	Addressed to the *digitally reluctant explaining* what happens to citizens' private information, even if they do not use digital tools	AUP
Privacy by design in privacy protection	The PbD test	Web page	informs users of how they may control their online information and retain confidentiality	AUP
	The PbD cartoon	cartoon for children	explains to children the basic tenets of privacy by design and what sort of embedded privacy choices they should look for when online	AUP
PbD in specific contexts	Work	Infographic/broshure	Privacy threats and risk management at work	AUP
	School		Privacy threats and risk management at school	AUP
	Transport System		Privacy threats and risk management in the transport system	AUP
	Smart spaces		Privacy threats and risk management in smart spaces	AUP
	Medical records		Privacy threats and risk management for medical records	AUP
Tools for Privacy Protection	Tor	Slides	An overview of Tor, including its origin, evolution, how it works, what it protects, its limitations, and possibilities.	AUP
	Blocking ads	Infographic/broshure	Which tools allow limiting the collection of data while browsing and reducing advertising	AUP
	Managing Privacy Settings		Focussed on social networks	AUP
EU Legal Order	Existing legal sources	Slides + reading material	The module describes the legislative initiatives that illustrate the state of the art in the EU legal order as well as the context within which they function	KU Leuven

ICT practitioners				
Subject	Module	Mode of presentation	Content	Contributing partner
PbD methodology PRIPARE	PRIPARE principles and concepts	Slides + select reading material	Introduce the PbD concept, the PRIPARE methodology, and its foundations, providing an overview of the related terms, and motivating ICT practitioners to adopt PbD approaches.	UPM
	PRIPARE methodology: Overview		Introduce the PRIPARE methodology and its steps.	UPM
	PRIPARE methodology: Privacy requirements engineering.		Describe the PRIPARE steps to move from privacy requirements to operational requirements.	UPM
	PRIPARE methodology: Privacy impact assessment and risk analysis	Slides + select reading material, templates, and examples of use	Describe the PRIPARE steps to carry out a Privacy impact assessment and a risk analysis.	UPM
	PRIPARE methodology: Best practices	Slides + select reading material, templates, examples of use, and a catalogue of best practices	Describe the best practices selected by PRIPARE, and how they can be applied within the PRIPARE methodology.	UPM
Privacy Patterns	privacy patterns	slides	In this module we introduce privacy design patterns, their possibilities and limitations.	UULM
Privacy Motivation	Failures in Privacy Systems	Slides, references to articles	In this module we are going to examine some examples of failures in privacy systems.	UULM
Privacy Strategies (see Hoepman: http://arxiv.org/pdf/1210.6621.pdf)	Minimise	slides, exercises	This module explains Hoepmans Minimise privacy design strategy, i.e., to restrict the amount of information that is being collected.	UULM
	Hide		This module explains Hoepmans Hide privacy design strategy, i.e., to hide informations and/or their relationship.	UULM
	Separate		This module explains Hoepmans Separate privacy design strategy, i.e., to distribute the processing of personal information to avoid the creation of personal profiles. (to discuss: there are perhaps no concrete technologies known to implement this approach)	UULM
	Aggregate		This module explains Hoepmans Aggregate privacy design strategy, i.e., to process personal data at the highest level of aggregation and with the least possible detail (group signatures, etc.)	UULM
	Inform		This module explains Hoepmans Inform privacy design strategy, i.e., it examines ways to inform the data subject over the data it	UULM

			provides and its use.	
	Control		This module explains Hoepmans Control privacy design strategy, i.e., it examines the ways, in which a data subject can control his or her data. (to discuss: this is perhaps too general)	UULM
	Enforce		This module explains Hoepmans Enforce privacy design strategy. (To discuss: This module perhaps has too much overlap with other modules over privacy policies. On the other hand it could add information about access controls)	UULM
	Demonstrate		This module explains Hoepmans Demonstrate privacy design strategy, i.e., ways for the data controller to prove that he complies with the privacy policy.	UULM
Location Privacy	Location privacy	slides, exercises	We introduce the topic of location privacy.	UULM
	Privacy in transport systems		We examine the role of privacy in transport systems and ways and technologies to achieve privacy.	UULM
Anonymous Cash			This module covers anonymous cash systems like eCash, DigiCash, etc.	UULM

Students				
Subject	Module	Mode of presentation	Content	Contributing partner
CS/Engineering Students				
PET	Privacy Enhancing Technologies and limitations	Reading list, pointers to existing material	Description of privacy preserving technologies including their capabilities and limitations.	WIT
Privacy in ICT environments	Understanding privacy	Reading list, + existing material,	Overviews of privacy basic concepts, its definitions and current related ethical problems and solutions.	WIT
	Privacy in the Internet of Things	Slides, exercises, reading list	Introduction to the Internet of Things and the emerging privacy issues involved.	AUP
	Privacy enhancing techniques for Web Services	Slides, exercises, reading list	Introduction to current web services, such as SOAP, WSDL, and REST and how they address privacy	AUP
	Secure programming		Technical description of how security and privacy related techniques are considered in programming practices.	WIT
	Security and privacy in software engineering		Introductions on building privacy and security into technology products and services and the related trade-offs. Integration of privacy protection and security into the overall engineering lifecycle of such products and services including requirements, design and testing phases.	WIT
	Web security and vulnerabilities		Descriptions of background issues in Web security and common vulnerabilities. The relationship of those vulnerabilities to user and consumer privacy.	WIT
	Cryptography		Introduction to cryptography techniques with references to detailed learning material particularly in relation to privacy.	WIT
	Security vs. privacy	Slides, exercises, reading list, pointers to existing material	Comparison and relationship between security and privacy concepts.	WIT
	Anonymisation	Pointers to existing material, text, video	Introductions and detailed discussions of anonymisation techniques.	WIT
	Security and privacy patterns	Slides, exercises, reading list, pointers to existing material	Description of design patterns that support security and privacy and references to more detailed discussions.	WIT
Database Privacy	Cryptography	Slides, exercises, reading list, pointers to existing material	Introduction to cryptography techniques for protection of data at rest with references to detailed learning material.	WIT
	Web and database		Descriptions of background issues in Web security and common vulnerabilities. The	WIT

	security and vulnerabilities		relationship of those vulnerabilities to user and consumer data privacy.	
	Privacy preserving data management	Reading list, pointers to existing material	Descriptions of privacy preserving techniques in data mining and processing and current limitations, such as scalability.	WIT
PbD Privacy risks and incidents	Security management	Slides, exercises, reading list, pointers to existing material,	Description of management of organisational privacy and security risks and the use of security metrics. Description of techniques to cope with privacy issues including identifying and dealing with privacy incidents and mitigating risks in the context of PbD. Overview of threat modelling techniques.	WIT
	Privacy Impact Assessment (PIA)	Pointers to existing material	References to existing PIAs and related discussions including its applicability to PbD.	WIT
	Compliance reviews		References to resources that describe and discuss issues around compliance audits and review techniques.	WIT
Cloud Privacy	Cloud privacy patterns and best practices	Slides, reading list	Introduction to privacy and security patterns applicable to the cloud environments and references to detailed discussions.	WIT
Mobile Privacy	Privacy issues in mobile devices	Pointers to existing material	Resources on privacy issues in existing mobile device platforms.	WIT
	Privacy vulnerabilities and solutions in Android	Slides, examples and exercises	An in-depth presentation of the issues mobile device's present and how the Android OS handles them with several examples and exercises	AUP
Economic Aspects	Trust and reputation	Slides, reading list, pointers to existing material	Description of the concepts of trust, trustworthiness and reputation as well as related systems and models.	WIT
NON-CS/Engineering Students				
History leading to PbD	History of technology related to PbD	Slides and exam questions	History of technology leading to the convergence underlying current privacy problems	AUP
	History of Human Rights related to PbD	Slides and exam questions	History of relevant human rights treaties and contemporary issues	AUP
Principles and processes of PbD	PbD: principles, processes, and operationalization	Slides and exam questions	regulatory view of PbD, PBD principles, PbD processes, PbD technologies, and current standard for operationalizing PbD	AUP
Application of EU privacy law online	EU regulation and privacy	Slides and exam questions	Current EU regulation and the debate around privacy and PbD in particular	AUP
Technology responses to privacy problems	PbD: perspectives and limitations	Slides and exam questions	How technology addresses privacy issues: perspectives and limitations	AUP

Legal and policy stakeholder				
Subject	Module	Mode of presentation	Content	Contributing partner
Data Privacy	Basic principles/ Relevant legislation	Slides + reading material	The module elaborates on the content of principle such as consent principle, data minimization (proportionality), and data quality, and its importance for the protection of the rights of the individual in the EU.	KU Leuven
Data Protection	Data protection reform		The module explains the reasons that triggered the data protection reform, analyses its content and discusses the major changes that are envisaged in the two proposals.	KU Leuven
PbD,: context	Part 1: How did the concept develop?		The module analyses how PbD developed in the EU and internationally. Of particular interest is the work of some European DPAs as well as of the EDPS that stressed the importance of the data minimization principle some time ago.	KU Leuven
	Part 1: How is PbD implemented in the draft regulation?		The module elaborates on how the draft regulation reinforces PbD.	KU Leuven
PbD,: design process	Part 1: Privacy risk management: data governance/ PIA/privacy risk management methodologies		The module discusses PbD within the general context of data governance.	KU Leuven
	Part 2: examples		Privacy by design in the field of cloud computing and biometric verification in border control. Each example follows a set four-part structure.	KU Leuven
	Part 3: How do legal principles affect policy making?		In this module privacy is perceived as a means to effective policy making. In the Commission Impact Assessment Guidelines (2009), privacy is a requirement that should be taken into account in the EU policymaking process.	KU Leuven