Teaching Privacy by Design to Non-Technical Audiences

Susan Perry[1], Claudia Roda[2]

[1] International Politics Department The American University of Paris, France
[2] Computer Science Department The American University of Paris, France
sperry@aup.edu croda@aup.edu

Abstract. As research in cyber security and privacy advances, privacy initiatives should be disseminated to the broader public. Education of this public is a key tool in conveying the seminal importance of security and privacy in our use of digital technology. This article presents a curriculum that, by targeting the non-engineering public, provides an opportunity for rapid acceptance of the innovative security and privacy research in which we are currently engaged.

Keywords: Privacy by design; Education; Curriculum.

1 Introduction

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 its benefits. This article explores the practice of joining two disciplines – law and science – in a university classroom in an attempt to understand more fully the dense, multidimensional nature of digital privacy. We demonstrate how privacy by design may be effectively taught to a combined group of undergraduate and graduate students in the social sciences whose knowledge of technology is limited to their own user experience. Our curriculum aims to explore a new educational space at the theoretical intersection of human rights and digital technology, while integrating a practical component that allows students to produce educational materials for stakeholder audiences; this merging of theory and practice provides our students with the opportunity to reflect on the convergence of law and science. We have designed our curriculum to address the salient need for privacy protection education for all sectors of the general public, as well as practitioners, regulators and students in related disciplines. The educational and reference material generated by the project targets the socio-ethical, legal and technical issues that privacy by design raises for these stakeholders across society.

The term "privacy by design" was coined by Ann Cavoukian, the Information and Privacy Commissioner for Ontario, since 1997, as a set of guiding principles in the design of computer software. Our curriculum incorporates her seven principles as core learning goals that enable students to practice privacy-by-design as they learn about it and

produce knowledge materials for other stakeholder groups. As will become clear in our paper, we believe that some of Cavoukian's principles are not limited to the context of privacy by design and can be effectively applied to other contexts at the interface of human rights and digital technology. Moreover, these principles have been used to support security by design [1]. Privacy-by-design principles include (1) proactive measures, (2) privacy as a default setting, (3) privacy embedded into design architecture, (4) transparency, (5) user-centric privacy measures, (6) functionality, and (7) end-to-end privacy implementation [2]. Although the definition of privacy by design through its seven principles has been, at times, challenged both for being difficult to operationalize and unclear [3, 4], we found that the seven principles form an excellent pedagogical tool for blending the technological and social aspects of privacy[1]. We will argue, however, that Cavoukian's functionality principle is somehow problematic, from a human rights standpoint, because human rights law stipulates a hierarchy of rights ranging from non-derogable to progressive that challenges Cavoukian's notion of win-win privacy, with no political or legal trade-offs. Our curriculum thus incorporates discussion of Cavoukian's principles into the teaching of a theoretical human rights framework for digital technology, along with the practical design of educational materials to raise awareness of privacy for stakeholder communities. The first part of this article explores the use of a human rights framework for understanding privacy by design, incorporating recent theory on participatory action research (PAR) as it applies to the university classroom [5]. The second part of this article presents our curriculum for the teaching of privacy by design, highlighting the originality of its combined focus on theory and practice. Part Three of this paper analyses the educational material produced by our students, the potential impact of this material on the broader stakeholder public, and how we may further develop privacy-by-design initiatives by the non-specialist community.

1 The Theoretical Framework for Privacy by Design

When Commissioner Ann Cavoukian and John Borking (representing then Commissioner Peter Hustinx) of the Dutch Data Protection Authority first presented their joint paper on Privacy-Enhancing Technologies in Brussels in 1995, they said "it was met with silence by the Commissioners in attendance" [6]. Since then, discussion has replaced silence and a range of scholarly literature has appeared to reinforce the principle of privacy by design in law and in practice. But, how were the theoretical underpinnings of Cavoukian's idea constructed? And what is the most effective method to foster a risk management culture that incorporates stakeholder concerns about privacy?

Privacy, as a right, is a relative late-comer to the pantheon of civil and political rights enshrined in the International Covenant on Civil and Political Rights (ICCPR). Warren and Brandeis' seminal article of 1890 treated privacy as a critical right, related to the full protection of person and property [7]. As the age of photography weakened control over one's personal image, the protection of intangible property and the right to prevent

[1] Note that the Office of the Information and Privacy Commissioner offers PbD educational material organized in two sets of slides aimed at introducing the concept to a large audience including "chief privacy officers, engineering instructors, social scientists, and privacy leaders". See http://www.privacybydesign.ca/index.php/publications/curriculum/

publication required legal protection that extended beyond intellectual property protection and protection from libel or slander [7]. The "right to be let alone" was thus linked from its inception with the right to prevent publication, an important factor when we consider the development of privacy by design as it relates to digital technology. The Universal Declaration of Human Rights, promulgated by the UN General Assembly in 1948, includes specific privacy protections in Article 12, taking up the ideas first expressed by Warren and Brandeis on the special protection of an individual's "honour and reputation" [8]. The ICCPR renders privacy protection legally binding in international law. General Comment 16, drafted by the UN Committee on Human Rights, focuses on the obligation of States to use legislative tools to protect their citizens' privacy: "this right is required to be guaranteed against all … interferences and attacks whether they emanate from State authorities or from natural or legal persons" [9]. Although the General Comment was promulgated in 1988, before the advent of the digital revolution, clearly the term "legal persons" is intended to mean businesses and consequently obliges States to guarantee the protection of user data by technology companies under their jurisdiction.

The ethical argument for privacy by design extends human rights law to the architecture and use of digital technology. Legal scholar Richard Posner argues that privacy is an overrated construct in a digital society [10], while sociologist Richard Harper views our trust in technology as an evolving paradigm [11]. We have argued that human rights can hardly be overrated, particularly when it comes to protection of the most vulnerable members of society [12]. Helen Nissenbaum's theory of privacy suggests that contextual integrity is at the core of what we consider privacy violations [13]. David Wright argues for a process of impact assessment that includes privacy and other human rights concerns [14]. Much of this scholarship addresses concerns that are also expressed by digital technology users, who indicated in a 2013 Pew survey a rising level of mistrust concerning data protection; according to the survey, "86% of internet users have taken steps online to remove or mask their digital footprints—ranging from clearing cookies to encrypting their email" [15]. The impact of the Snowden revelations, along with a rich trove of user anecdotes concerning online privacy violations, have led users to demand greater control over their online data.

Regardless of whether this high level of user mistrust concerning privacy protection of digital information is justified, international human rights law and the fairly robust Data Protection Regulation proposed by the European Commission on 25 Jan 2012 require protection of online privacy. In guiding our students to produce educational materials for various types of stakeholders, we have focused on the practical problem of how best to implement the right to privacy on a day-to-day basis. Providing an already mistrustful population with privacy-enhancing knowledge and tools is a seminal example of the mis en oeuvre of participatory action research methods [5]. PAR is based on the ideas of engaged inquiry and democratization of knowledge, where research is done with the concerned subjects rather than on or for them. Our curriculum thus attempts to provide privacy-by-design constructs as part of the organizational basis for course activities, as well as the content focus of the actual materials produced – a way of engaged inquiry and knowledge democratization that echoes the founding discourses of the Internet itself – a free and open space for the development of people everywhere (see [16]).

2 Integrating Privacy by Design into a University Curriculum for the Social Sciences – the Seven Principles

Our curriculum is designed as an interdisciplinary study of the rich intersection between human rights and digital technology. Each of Cavoukian's seven principles is addressed through the lens of a case study, with issues selected on the basis of their cross-cutting impact. It should be noted that our curriculum does not address these principles in order, but proposes a slightly different arrangement that allows for greater pedagogical cohesiveness. Approximately two-thirds of classroom time is dedicated to lectures and discussion, with the professors and visiting lecturers, while one third is devoted to developing privacy-by-design educational materials for stakeholder communities. The interaction between theory and practice, or analysis and production, privileges participatory action research, enabling students to engage in meaningful inquiry and to model the dissemination of their own knowledge. Students evaluate the course qualitatively and quantitatively at the end of the semester, and these evaluations are an important tool for improving course content and delivery, as well as fine-tuning curricular details.

2.1 Full Functionality — Positive-Sum, not Zero-Sum

Our curriculum begins with an overview of the histories of human rights law and digital technology from 1945 to the present. In many respects, we are virtual tightrope walkers, precariously balancing two remarkable acquisitions of the post-Cold War period: the simultaneous development of the formal international human rights framework and the informal network of information technologies. The promulgation of binding treaty law for the implementation of human rights has accelerated since the end of the Cold War, alongside the proliferation of multiple channels of communication offered by the growth of information technology. This dual paradigm has created new tensions between individual citizens and their States, one that reinforces shifting political patterns. We encourage our students to reflect on how the human rights framework, on a national and international level, interacts with digitally-driven networks to provide citizens with leverage to safe guard their rights. And yet, as digital technology users learn to intervene in governance in a myriad of innovative ways, governments and companies are using the same technology to interfere with human lives on a brand new scale, both for better and for worse. It is the dense, contested nature of this interaction that creates the potential for greater democracy or more abject tyranny.

We take issue with the idea that human rights protection of digital technology users is a win-win equation for all concerned. On the one hand, rights protection may be expensive for governments or business to implement, but such protection reinforces the social contract that underpins democratic governance and provides an ethical legitimacy for political and corporate actors. On the other hand, discrimination, violence against women and environmental pollution are expensive to society, and could be mitigated through timely implementation of human rights law. Our curriculum encourages students to identify the trade-offs that occur as new technologies are regulated, or not regulated, by the public sector. We emphasize that no public or private actor is above

the law or the general public interest, hence functionality may not apply in all circumstances.

We conclude by stressing how the issue of privacy has been, and will continue being, a multifaceted problem that both creates a variety of different expectations amongst stakeholders and affords multiple technical solutions. We explore the diversity of privacy paradigms that populate the online experience (e.g. control, confidentiality, practice [17]) highlighting the user perspective [18]; we compare the regulatory frameworks currently applied in various countries with a focus on Europe and US law (e.g., [19]) and introduce several privacy enhancing technologies, explaining their role in embedding privacy into digital systems [20, 21].

2.2 Proactive not Reactive; Preventative not Remedial

In addressing the issue of proactive measures, we examine a pervasive element of the digital revolution that suffers from a lack of proactive, or even remedial regulation: the hardware that makes the digital revolution possible. Fascination with wireless technology – the sleek design of smartphones and tablets, the dizzying range of applications and available information, the ability to be "connected" at all times – has blinded the general user to the potential costs of the hardware necessary to make the technology function. There are over five million mobile phone towers worldwide, for example, serving 96% of the global population through the provision of electro-magnetic waves (EMF), a low-frequency form of radiation [22]. This "invisible" infrastructure constitutes one of the largest experiments with human biology and environmental capacity to date, and yet scientists are still debating how to measure its impact and how to evaluate the long-term consequences of electromagnetic wave exposure on the human organism [23]. Class discussions indicated the extent to which our students had never reflected on the levels of electricity required for the storage of digital data or the electromagnetic wave emissions necessary to make their smart phones function. This curricular unit is designed to provide students with a lay-person's understanding of EMF science, the controversies over EMF measurement and its impact on living organisms, and the human rights paradigm that requires proactive application of the precautionary principle. By applying Cavoukian's first principle to an often-ignored aspect of the digital revolution, we enrich the argument for proactive regulation and extend the case to protection of human health and the environment.

2.3 Privacy as a default setting

In "Integrating privacy and ethical impact assessments", David Wright and Michael Friedewald argue for an ethics of design, the application of a human rights framework to software production before the rollout of the final product [24]. This curricular unit provides students with an understanding of the potential ethical controversies surrounding software design. We invited David Wright into our classroom to discuss with students his evaluation of both the privacy enhancing technologies we use, as well as the application of binding human rights treaty law in the very design of every IT product. As his work makes clear, privacy would be a default setting if a privacy impact

assessment were properly applied in all circumstances. Our students were particularly intrigued by the potential for cross-cultural and political application of Wright's system of ethics: who should determine the framework of a PIA – governments, companies or users? Is Wright's ethical impact assessment [25] a strictly Western construct, or could it be applied to protect privacy in an authoritarian state? Could a PIA be used for political or economic purposes to prevent the design or delivery of new IT products? How will freedom of expression be impacted if privacy is the default setting? These and other questions extended discussion of Cavoukian's principles to the larger realm of human rights and their universality.

2.4 Visibility and Transparency — Keep it Open

Our classroom discussions indicated that the issue of censorship strikes a chord with our students, all of them sensitive to the precarious balance between national security and citizen privacy, as disclosed by the Snowden revelations. Policy transparency, whether it be focused on spying or on censorship, is another lens through which to examine the idea of a free and open Internet. We use China as an example of the tensions between users determined to pursue online freedom of expression and a government bent on forestalling the possibility of organized street demonstrations facilitated through social media [26]. The closed system of the Chinese Internet, with copycat search engines (*baidu*), Twitter (*weibo*), and WhatsApp (We Chat or *weixian*), is an ideal laboratory in which to explore the contradictions inherent in the principle of Internet freedom versus the need for governments to monitor online citizen activity to prevent crime and terrorism. It is hardly a surprise that the Chinese Party-State has built a Great Firewall in an effort to keep online protest from spreading to the streets, a seminal concern in a nation that already experiences a significant number riots, or "mass incidents", per year[2]. Our curriculum encourages students to examine the reasons for government control of the Internet, and to weigh the importance of a series of violations ranging from freedom of expression to private property to privacy. We examine government censorship and user-driven self-censorship, as well as clever tools designed to circumvent censorship, such as the "grass mud horse" lexicon, a humorous set of character puns developed by Chinese netizens. Students are encouraged to think about the impact of censorship on privacy by design; privacy as a default setting is a weak concept unless bolstered by a visible and transparent privacy protection policy within a strong legal framework, such as the recently proposed Data Protection Regulation.

2.5 Privacy Embedded into Design

The Internet of Things (IoT), a diffuse concept that embraces the connection of objects to one another and to humans, is of particular importance to an audience of general users. We have structured this curricular unit to focus on the potential ubiquity of

[2] The Chinese government last published the number of annual mass incidents in 2005. Anecdotal speculation brings the number to as high as 180,000 riots per year - see Freeman, Will (2010) The Accuracy of China's mass incidents. Financial Times, March 2.

privacy violations in a world where things are more connected than people. Starting from a list of six European Union concerns regarding the IoT [27], we examine issues such as trust, agency and autonomy in the context of privacy and the Internet of Things. Both hardware and software violations come to the fore, as students analyse the advantages and disadvantages of a fully digitized world. Our curriculum encourages students to evaluate who would be most vulnerable to privacy violations – the poor who lack regular access to a digitized environment, employees whose work and physical presence may be assessed via digital monitoring, the elderly who rely on assisted living technologies – and how this might matter. Is it possible to successfully embed privacy protection into all design and how is the user to express the level of desired protection, or to know whether such options exist? Our students quickly took the discussion one step further to ask what other human rights protections are challenged by the Internet of Things?

2.6 End-to-End Security — Full Lifecycle Protection

This course unit asks the students to consider the different stages of design, implementation, deployment, maintenance, upgrading and disposal of both simple and complex systems. As users, our students rarely consider this whole lifecycle or the complexity associated with systems that integrate different components. The objective is to highlight that privacy can only be achieved by taking appropriate measures across system components and throughout the whole lifecycle. We draw on the example of privacy protection in the charging procedure for electronic vehicles. This procedure, if not appropriately designed, may reveal to charging station and mobility operators unnecessary information about users' locations and possibly other personal data. Our students were introduced to the design of a protocol addressing the communication between the charging station and the vehicle baptized 'Popcorn' by its creators [28]. This specific example is particularly interesting because the procedure followed by the authors of Popcorn clearly shows how privacy impact assessments may be used both to derive design requirements and to assess the level of privacy protection of the solution. We invited scholar and protocol team member Frank Kargl to illustrate the privacy issues addressed by the protocol and explain, to our non-technical audience, the privacy enhancing technologies (PETs) supporting the system. Professor Kargl argued that e-mobility through ad-hoc, needs-based electric car rental, particularly in urban areas, is considered one of the next milestones for the automotive industry. But, connecting electric cars to a power grid without storing data on user identity, mobility or payment methods is a challenge. This curricular unit follows our work on privacy as a default setting and embedded privacy, allowing students to explore the practical implications of privacy protection in their daily lives. The success of Popcorn in protecting user privacy demonstrates that human rights protection is often an issue of creative thinking.

2.7 Respect for User Privacy — Keep it User-Centric

This principle is explained as "Respect and protect interests of the individual, above all" [1] and requires a clear identification of users and their needs. We encouraged our students to reflect on users and their needs by asking them to design educational

materials on privacy for a variety of stakeholder communities. Few guidelines were issued to students. Thanks to the small class size typical of liberal arts institutions, we were able to establish groups of no more than five students, each with an assigned target audience: the general public; the digitally reluctant; children; EU regulators not working on privacy; national regulators not working on privacy; and human rights advocates. None of these audiences can be considered specialists on privacy issues. Students were given the option to make their final product available to the Creative Commons, following a discussion of copyright protection and whether the Creative Commons offered an opportunity to impact political discourse on the issue of privacy protection. They presented their projects to their classmates on two occasions in order to receive peer feedback, and submitted four drafts for our comments before handing in their final project in electronic form. In our determination to empower our students, we underestimated their initial sense of panic caused by the lack of detailed guidelines. Nonetheless, within three months, our students demonstrated, through their production of rich, yet streamlined educational material, a mature understanding of the theoretical convergence of human rights and digital technology as manifested in online privacy issues.

3 Student Production of Educational Materials for Privacy by Design

In this section, we provide two examples of student production of privacy-by-design educational material, one for the general public (produced by a group of graduate students) and one for children (produced by a group of undergraduates). Both samples represent patterns that we noted across student submissions: (1) the incorporation of their own user experiences into the design of educational materials; (2) a commitment to striking visual design; (3) a sophisticated awareness of the Internet as a public good, an online extension of their "heterogeneous and thickly integrated" social lives [13].

Figure 1 presents the first page of a two-page, student-produced infograph that synthesizes online and offline life in a realistic manner, visually demonstrating the blended characteristics of a typical student day. In addition to the visual sleekness of the sample, we note the contextual integrity suggested by Nissenbaum, a seamless transfer of offline activities to online platforms [13]. This sample also demonstrates our students' understanding of the theoretical integration of individual human rights with the possibilities for privacy violations inherent in digital technology use, and the provision of recourse for privacy violations. It is possible that our choice of a participant action research methodology may have led our students to think in terms of PbD as a legal or technical recourse, to render more robust their assessment of commonly-occurring violations.

The second knowledge product (Figure 2) is a cartoon that focuses on the protection of minors from cyber bullying; the cartoon was drawn from a student-produced magazine addressing children and their parents. According to the Australian government, the most vulnerable age for this form of harassment is 14-15 years old, the group targeted by this cartoon's school setting [29]. Again, participant action research methods may have encouraged our students to privilege their own personal experiences

in a carefully constructed design that provides recourse, in this case reporting the incident to parents and the use of a hotline. The choice of a colorful design and two female characters was carefully thought through, as was the extreme simplification of the message and the pitch for privacy as a default setting. Both Figure 1 and Figure 2 are aimed at a general public that is unfamiliar with privacy by design as a concept, or the idea that privacy could be a default mechanism on social media sites. This should be the starting point for educational materials on privacy, since all sectors of society must be brought on board if privacy is to become the default setting expected by the general public when using the Internet, or purchasing digital objects and software.

Conclusions

By working closely with six student teams over the course of the semester, we were provided with a window on the thinking of the general user. Non-engineering students who spend an average of two-three hours a day online are ideally situated to design knowledge products that promote online security and privacy amongst the general public. The condensed analyses embedded in their knowledge products is a reflection of the curriculum's assigned readings, lectures and discussions that bring together law and science in an effort to explore the Internet as it impacts their lived experience. By transferring privacy principles to the larger domain of human rights and digital technology, our students were able to view security and privacy protection as part of a larger exploration of how we are going to live in a digitally connected society. Only by privileging the broader perspective can we deliver on the promise of digital technology to enhance democratic dialogue and facilitate human lifestyles, and make sure that it is safe to use for the generations to come.

References

1. Cavoukian, A., Dixon, M.: Privacy and Security by Design: An Enterprise Architecture Approach. (2013) Retrieved 10.5.2014 at http://www.privacybydesign.ca/index.php/paper/privacy-security-design-enterprise-architecture-approach/
2. Cavoukian, A.: Foundational Principles (Privacy by design). (1997) Retrieved 22.5.2014 at http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/
3. Rubinstein, I., Good, N.: Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. Berkeley Technology Law Journal August 2011, 4
4. Gürses, S., Troncoso, C., Diaz, C.: Engineering Privacy by Design. International Conference on Privacy and Data Protection (CPDP), Belgium (2011)
5. Reason, P., Bradbury, H. (eds.): Handbook of action research. Sage Publ, London (2013)
6. Cavoukian, A.: Privacy by design: the definitive workshop. A foreword by Ann Cavoukian. Identity in the Information Society 3, 247-251 (2010)
7. Warren, S., Brandeis, L.: The Right to Privacy. Harvard Law Review IV, (1890)
8. Universal Declaration of Human Rights: G.A. Res. 217 A(III), adopted by the U.N. Doc. A/810 (December 10). (1948)
9. Office of the High Commissioner for Human Rights: CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. Adopted 8 April 1988. (1988)

10. Posner, R.: Privacy is Overrated. New York Daily News. 28 April (2013)
11. Harper, R. (ed.): Trust, Computing and Society. Cambridge University Press (2014)
12. Perry, S., Roda, C., Carlson, K.: Submission United Nations Committee on the Rights of the Child - General Comment on the Rights of the Child and the Business Sector (2012)
13. Nissenbaum, H.: A Contextual Approach to Privacy Online. Daedalus 140, 32-48 (2011)
14. Wright, D., Finn, R., Gellert, R., Gutwirth, S., Schütz, P., Friedewald, M., Venier, S., Mordini, E.: Ethical dilemma scenarios and emerging technologies. Technological Forecasting and Social Change forthcoming,
15. Pew Research Internet Project: Anonymity, Privacy and Security Online. (2013) http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online-2/
16. Internet Society: Internet Society Mission Statement. (2014)
17. Diaz, C., Gürses, S.: Understanding the landscape of privacy technologies. Information Security Summit (2012) http://homes.esat.kuleuven.be/~cdiaz/activities.html (1.5.14)
18. Jutla, D.N.: Layering Privacy on Operating Systems, Social Networks, and Other Platforms by Design. Identity in the Information Society, IDIS 3, 319-341 (2010)
19. Schwartz, P.M., Solove, D.J.: Reconciling Personal Information in the United States and European Union. California Law Review Forthcoming, (2014)
20. European Commission: Communication on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007) 228 final, Brussels, 2 May 2007. (2007)
21. Goold, B.: Building It In: The role of Privacy Enhancing Technologies in the regulation of surveillance and data collection. In: Goold, B., Neyland, D. (eds.) New Directions in Surveillance and Privacy. Willan, Devon (2009)
22. International Telecommunication Union: ICT Facts and Figures. (2013) http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf (26.9.2013)
23. Roda, C., Perry, S.: Mobile phone infrastructure regulation in Europe: Scientific challenges and human rights protection. Environmental Science & Policy 37, 204-214 (2014)
24. Wright, D., Friedewald, M.: Integrating privacy and ethical impact assessments. Science and Public Policy 40, 755–766 (2013)
25. Wright, D.: A framework for the ethical impact assessment of information technology. Ethics Information Technology 13, 199–226 (2011)
26. Perry, S., Roda, C.: Conceptualizing and Contextualizing the Changing Nature of Internet Usage in China. China and the New Internet World: The Eleventh Chinese Internet Research Conference (CIRC11), Oxford Internet Institute, Oxford (2013)
27. van der Hoven, J: Fact Sheet – Ethics, IoT Expert Group. European Commission. (2011) http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1751 (10.5.2014)
28. Höfer, C., Petit, J., Schmidt, R., Kargl, F.: POPCORN: Privacy-Preserving Charging for eMobility. First Workshop on Security, Privacy and Dependability for CyberVehicles (CyCar) at 20th ACM Conference on Computer and Communications Security (2013)
29. Australian Ministry of Education Safe Schools Hub: "What is cyberbullying?". http://safeschoolshub.edu.au/for-parents/what-to-do-about-/staying-cybersafe/what-is-cyberbullying- (22.5.2014)

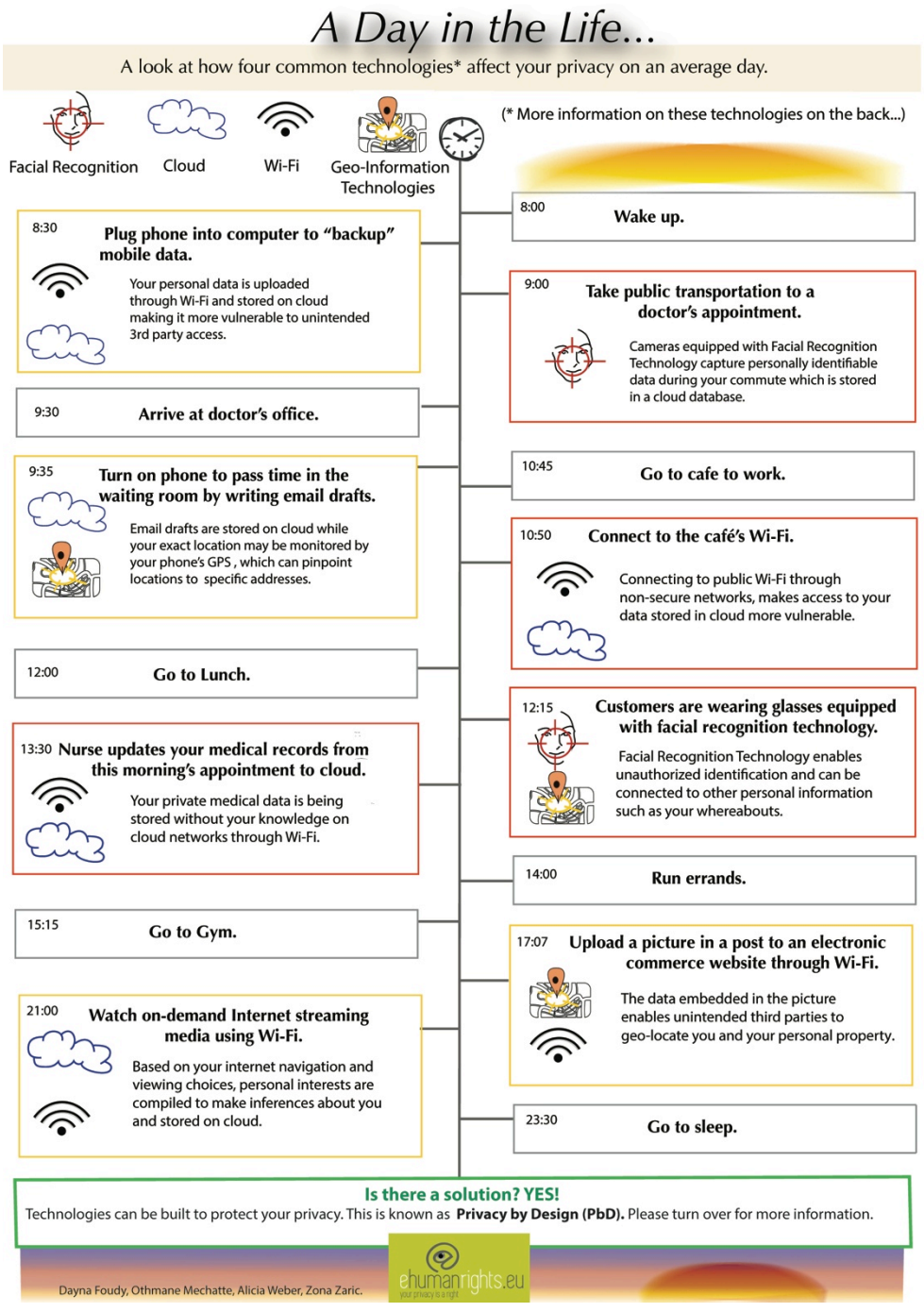

Fig. 1. First page of general public infographic.

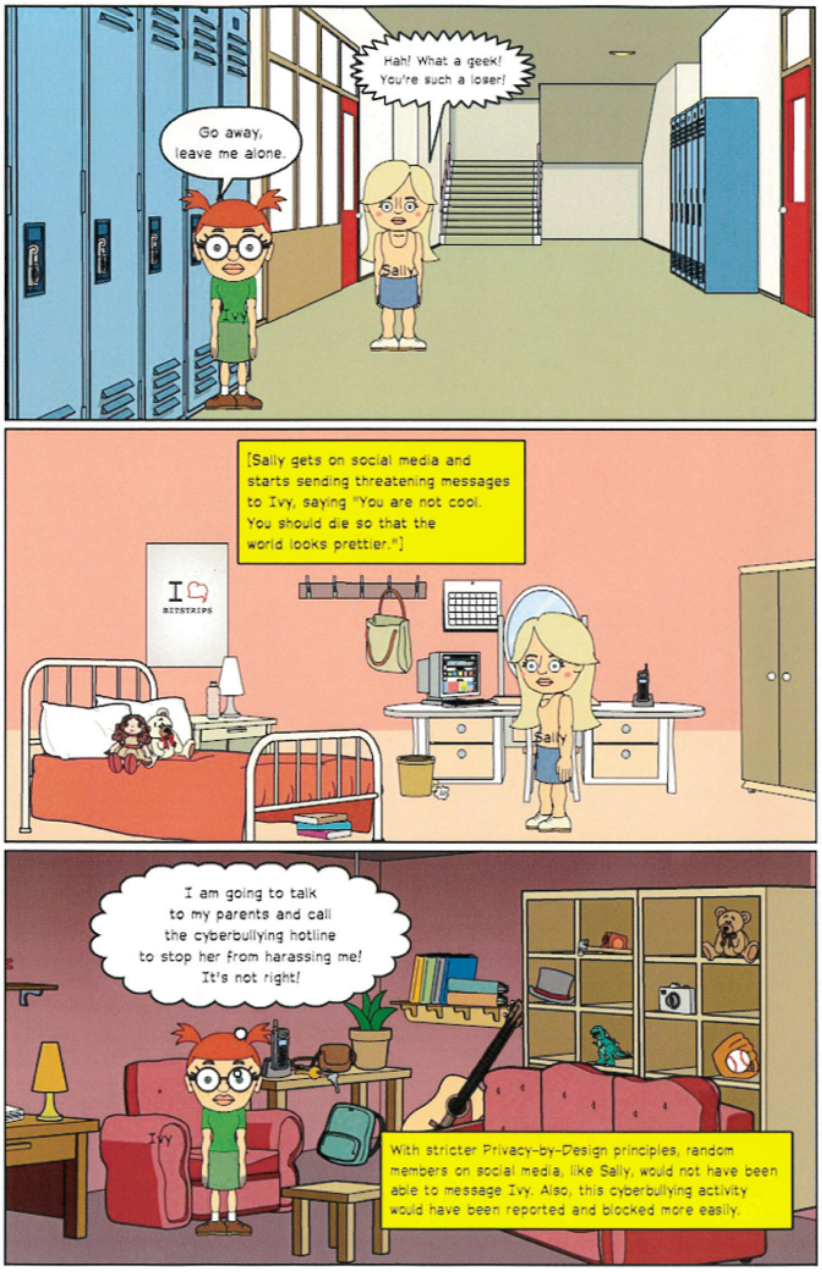

Fig. 2. Extract from information booklet for children.