WHAT DO IT PROFESSIONALS THINK ABOUT SURVEILLANCE?

Ivan Szekely

DRAFT

to be published in

Christian Fuchs, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval (eds.)
Internet and Surveillance. The Challenge of Web 2.0 and Social Media.
New York: Routledge, 2011

A sceptic reader might be tempted to fire back with a "Who cares?" Surveillance exists and is becoming more widespread, independent of what the experts think.

In addition to presenting the findings of a recent research and interviews with IT professionals on such issues as surveillance and the handling of personal data and privacy in general, the author's intention has been to frame an argument in favour of making IT professionals' views on these matters count more in the formulation and implementation of the concept of modern surveillance systems.

Another interesting aspect of the topic is that, insofar as research on privacy is concerned, the IT community constitutes something of a white area and, therefore, our conclusions may enrich the discussions on the subject with some novel viewpoints, hopefully leading the emergence of new policies, strategies and areas of intervention for the benefit of the numerous stakeholders. The immediate motive for writing this paper has, however, been supplied by the BROAD project: a recent research that employed quantitative and qualitative methods alike, which was designed to test the views, the knowledge and the attitudes of IT professionals.

Finally, our paper also wishes to call attention to the importance of the empirical approach by pointing out that, in addition to the purely theoretical constructions, the direct study of reality could also help galvanize the speculative methods and engender further interactions between theory and practice.

1. Introduction

Once we subscribe to Lessig's (2000) famous view whereby "the Code is the law" in modern information societies, it will follow directly that the coders are the lawmakers in today's society. And if they are indeed the lawmakers, they are likely to produce laws that will reflect their own views, depth of knowledge and attitudes – naturally, alongside the views of their paymasters. This system has certain boundary conditions, such as the economic interests and the legal regulations, but those will merely shade the views of the IT professionals, rather than defining them. Experience tells us that the law in general – despite its fundamental role in mediating values – seem to carry very little weight with the IT professionals, who tend to regard them as useless restrictions.

Naturally, the law cannot simply be envisioned as the sum total of abstract rules, as the law must, at some level, relate to the underlying values that determine the workings and the conditions of a society. [1] The individual societies may differ with regard to the closeness and transparency of this relation: it is stronger in legal systems steeped in the traditions of natural law, and weaker in countries preferring a positivist approach. In the case of data protection laws, or in a broader sense privacy laws, the value content is clearly reflected in those internationally accepted legal principles that form the basis of national and international legal documents.

[1] See for example Dyzenhaus et al. (2007)

Therefore, if one is to discover what factors are likely to influence the views of IT professionals, one should first have to find out about the depth of their knowledge on data protection or privacy legislation, independent of the actual views they hold about it. Naturally, one would have to learn a great deal more about the members of this professional group, before one could form a picture about the views they have on surveillance, enhanced or in some cases generated by today's ICT, as well as about the subjects of surveillance and the handling of their data. We must learn about their views on social values, with special emphasis on the ways of their realization in today's ICT environment; we must discover their opinions on data subjects, the users of Internet services, their colleagues and even themselves. And if we want to extend our research into the causes that give rise to these specific "laws" of information society, we should also study the micro-environment and operational structure in which IT professionals work.

But first we must settle one fundamental question: Who qualifies as an IT professional? Or in a broader sense, who qualifies as an "informatician"? Is it any person who engages in some areas of informatics in ways that are beyond the capacity of an ordinary user? These terms have been slow to strike root in the English usage; although the word "informatics" has by now gained general currency, it still smacks of its French origin, l'informatique. And anyone who works in informatics can at best be called an informatician2, or perhaps more appropriately an information technologist or an information scientist. The scope of the present paper would not allow the author to analyze the substantive differences between the Anglo-Saxon and the Francophone terminology; nevertheless, we must find a way to draw the boundaries of our research subject.

If we want to limit our study to the circle of IT professionals, then we must be able to define the range of people who belong to that circle. So who is an IT professional? Anyone who has received formal IT training? Anyone who works in IT-intensive jobs? Anyone who is a member of any professional organization? Or anyone who considers himself or herself an IT professional? According to the definition provided by Wikipedia:

> "IT professionals perform a variety of duties that range from installing applications to designing complex computer networks and information databases. A few of the duties that IT professionals perform may include data management, networking, engineering computer hardware, database and software design, as well as the management and administration of entire systems." [3]

We must bear in mind, however, that a social group thus defined possesses neither a central registry nor a coherent pool of statistical data and, therefore, its members can only be reached through indirect methods, with the result that our population sample in no way can be regarded as a representative one. When we designed the BROAD project, which will be presented in detail later, we decided that instead of striving for representativeness, we would try to identify the characteristic groups of the IT community, engage them in our

[2] In the author's own definition, a "social informatist" – even if this expression cannot be found in any of the English dictionaries.
[3] http://en.wikipedia.org/wiki/Information_technology

research and base our conclusions on their views. In order to select from the vast toolbox of social science studies those elements that are methodologically suitable and practically viable and can empower us to put forward relevant statements on the views of IT professionals, we had to resort to qualitative and quantitative tools alike.

Naturally, we also had to take into account those research preliminaries, which either could serve as reference points for our study or will help to prove that our project has filled a gap in this research area.

2. Research preliminaries

First it should be noted that a large part of the papers on surveillance are studies conducted from a criminology or law enforcement angle, which means that they tend to take a positive view of surveillance, with an aim to develop efficient strategies to further the social acceptance of surveillance. Some of these studies justify the need for surveillance by drawing general conclusions from cases, which, from the viewpoint of law enforcement, have been perceived as success stories (Hanna and Mattioli 1995, Clark 2009); some others legitimize the practice by analyzing the laws that regulate surveillance (Figliola 2007); while others still talk about the natural marriage between law enforcement and the surveillance industry (Enright) – to name but a few examples. We have not covered these studies, partly because instead of taking such a particularistic view we wish to approach the subject of surveillance in a much more general manner, and partly because – while we have done our best to remain objective according to all the rules of our profession – we, the author and his colleagues, consider the prospect of the surveillance society (or its special category, the actuarial society) an unwelcome development, which has numerous negative aspects. One such negative aspect is the growing information gap between the observer and the observed; another one is the tendency whereby individuals living in such societies are becoming less and less capable of controlling the fate of their personal data and increasingly lack the capacity to see the impact that these data can have on their lives. Similarly negative, in our opinion, is the approach, which prefers a treatment of symptoms to the addressing of the root causes by perceiving everyone as a potential deviant who needs to be placed under constant surveillance.

The research preliminaries included in our study belong to the category of either an area known as surveillance studies4 or the broader field of privacy studies. We concluded that in most of the cases such studies either take the entire population as their research subject, or focus on some easily identifiable segments, such as young people, the consumers, the Internet users or the students. With sporadic exceptions, IT professionals as a group have not been investigated in these studies. [5]

[4] By now, this multi-disciplinary field has produced a number of highly acclaimed research and learning centres, such as the Surveillance Studies Centre at Queen's University (Kingston, Canada) and City University London, which runs an MA course in Surveillance Studies; the academic field has a prestigious professional forum in the Surveillance and Society Journal, and its researchers and research centres can keep in touch through Surveillance Studies Network (http://www.surveillance-studies.net).

[5] One part of the available studies deal with computer ethics or organizational ethics in general, which may include privacy- or surveillance-related aspects with regard to the views and behaviour of IT professionals. In this category the study of Collins and Stahl (2002) deserves particular attention, in which the authors analyse the

Globalization of Personal Data (GPD), one of the most important empirical studies of recent years, was conducted by the Surveillance Studies Centre of Queen's University. The multi-country survey covering Brazil, Canada, China, France, Hungary, Mexico, Spain, the US and Japan[6], which involved nearly 10,000 respondents, targeted the general population, or the population of telephone users, to be precise.[7] However, the telephone penetration rate is so high in the countries concerned (with the exception of Brazil, China and Mexico) that this imposed no special filter on the selection of respondents. This was a pioneering project, not only because of its cross-country and cross-cultural aspect, but also in the sense that instead of settling for the recording of the respondents' views, it also probed the depth of their knowledge, as well as their attitudes, values and beliefs with regard to surveillance and information privacy. To achieve this, they conducted qualitative focus group interviews in each country prior to their survey, which was analysed quantitatively.[8]

At this point I would like to note that, with regard to the Hungarian data, which was of special interest to the author, the findings of the GDP research provided further evidence for the existence of the threshold of abstraction, a concept introduced by the author (Szekely 2010, 167-168). It is well known to researchers conducting empirical studies that face-to-face interviews often yield opinions and attitudes that are different from those obtained through survey-type questionnaires from the same respondents. This is partly explained by the fact that the survey-type questionnaires, and most notably those related to surveillance and the handling of personal data, tend to use abstract concepts and refer to abstract situations, the actual content and relevance of which the respondents can comprehend only after receiving detailed explanation, and so the two methodologies yield different opinions. Among others, the acknowledgment of this led the planners of the BROAD project in their decision to complement the online survey with a series of semi-structured face-to-face interviews in two countries.

Therefore, the GDP survey targeted the total population, and we cannot extract the data of IT professionals from this sample because of the incomplete information regarding the respondents' occupation.

Another major empirical study completed in recent years was the survey conducted under the aegis of PRIME[9], a project involving nearly 8,000 respondents from three countries, first and foremost The Netherlands (Leenes and Oomen 2009).

---

moral problems of employee surveillance and the role of codes of conduct in influencing the behaviour of IT professionals within the organization. Studies have also been published about the potential risk posed by the IT professionals to the security of the organization, such as the annual "Trust, Security and Passwords" survey and analysis prepared by Cyber-Ark Software (2007–2010), implicitly suggesting that IT professionals themselves should be kept under surveillance.

A significant exception to the negligence of researchers in the area of exploring IT professionals' own views about surveillance and the management of personal data in general is Shaw's empirical study of webmasters' attitudes (2003), the findings of which we shall refer to in the following.

[6] The data collection project conducted simultaneously in eight countries in the summer of 2006 was extended to Japan in December 2007; however, the (online) methodology used in the latter country was different.

[7] The survey interviews in Canada, France, Hungary, Spain and the US were conducted over the phone by professional pollsters.

[8] The results of the research have been published in a book (Zureik et al. 2010).

[9] Privacy and Identity Management for Europe (PRIME) was a project supported by the European Comission's Sixth Framework Program (2004–2009) aimed at developing privacy-enhancing identity management solutions (http://www.prime-project.eu). As part of the project, the Tilburg Institute for Law, Technology, and Society (TILT) lead empirical research on user attitudes relating to privacy.

The PRIME survey focused on users' attitudes with regard to trust, privacy, the handling of personal data and PETs (Privacy Enhancing Technologies). One of the most interesting developments in connection with the survey was that, based on its findings, Oomen and Leenes (2008) created a privacy risk perception index, which offered an alternative to the well-known – and, in its critics' views, somewhat oversimplified – Westin/Harris Privacy Segmentation Index (Harris Interactive 2001).10 Despite its interesting conclusions and methodological thoroughness, the PRIME survey can be taken as a research preliminary for the BROAD project only in a limited sense. The PRIME survey studied a particular segment of the population, namely higher education students. It approached 388 universities and colleges from three countries – Belgium (Flanders), The Netherlands and the UK – and their students made up the survey's respondents. While the respondents included students studying IT related subjects, their views were not separated within the study. Although it would be possible to conjecture the character of training from the respondents' educational background and university, any comparison with the BROAD project's sub-sample, the IT students, would only have limited usefulness.

The only widely known survey focusing on a particular segment of the community of IT professionals is described in detail by Thomas R. Shaw (2003). In his research work, Shaw studied the attitudes of the webmasters of the world's most visited websites in relation to their decisions affecting the private lives of the users, as well as the their considerations behind these decision. Although his population sample was relatively small in a statistical sense11, his hypotheses and methodology were noteworthy. Shaw conducted his investigations on the basis of the theory of moral intensity. Out of the six dimensions of the theory12, he found two to be applicable: those of the magnitude of effect and the social consensus. He complemented the theory with the indicator of proximity, which turned out to be crucial from the viewpoint of organizational consensus and moral attitudes. (The role of the organizational consensus was also studied in the BROAD project.)

Similarly noteworthy was the methodology Shaw used, as he substituted the study of actual behaviour with the study of attitudes on the basis of the theory of reasoned action, developed by Fishbein and Ajzen (1975). He had twofold reasons to do this: first, the behaviour of the respondents was not easily observable in the given survey situation; and second, self-reported behaviours tend to provide unreliable data. At the same time, the attitudes were directly related to both the moral decisions and the actions arising from them, so they were suitable as substitutes for the direct observation of behaviour. On top of that, in comparison to the rate of technological developments, the attitudes can be described as relatively stable phenomena and, therefore, they provide suitable material for the prognostication of behaviour in the environment of future technology.

[10] For a critical analysis, see Kumaraguru and Cranor (2005) or EPIC (http://epic.org/privacy/survey)
[11] From the nearly five thousand webmasters successfully reached through e-mails, Shaw received a total of 359 usable responses (Shaw 2003, 309).
[12] Magnitude of effect, social consensus, probability of effect, temporal immediacy, proximity, concentration of effect. (Jones 1991)

3. The BROAD project

Carried out by Dutch and Hungarian educational and research institutions (2009–2010),[13] the project Broadening the Range Of Awareness in Data protection (BROAD)[14] has three main action areas: to study the views of IT professionals and to provide feedback to the people concerned; to develop an Internet platform for sharing knowledge and opinions about PETs;[15] and to produce creative artworks to increase people's awareness of surveillance and other privacy evasive phenomena.[16]

The action area designed to study the views of IT professionals (Survey and Feedback) was led by Tilburg Institute for Law, Technology, and Society (TILT), which is part of Tilburg University. The research consortium's work was actively supported by its two Hungarian members, the Central European University and the Eotvos Karoly Policy Institute.

The objective of this activity was to explore in Hungary and in The Netherlands the opinions, values and attitudes of the target groups that exert a decisive impact on the possibilities and limitations of people's privacy in today's "information society" (multipliers); and to feed back the results to the target groups and common knowledge. To achieve this objective, (a) face-to-face interviews and (b) a dedicated online survey were conducted in two specific target groups in both countries:

1. IT professionals (including the ones who work in explicit rights-restricting areas such as surveillance systems, border control etc.) – in other words, those who are *making* (designing and operating) IT systems processing personal data; and
2. Principals, i.e. those who are *commissioning* these systems and paying these IT professionals, namely
   (i) bureaucrats and decision makers, and
   (ii) business managers of service providers and operators, including small and medium enterprises (SME)

4. Hypotheses

We started out from the following general hypotheses, which we have advanced partly on the basis of our study of the source materials and partly as a result of our lead researchers' practical experiences deriving from working with information technology professionals for decades:

(1) The opinions, values and attitudes of IT professionals and their principals have a decisive impact on the IT systems they create and maintain for processing personal data; thus this has a direct impact on data protection/information privacy of the data subjects; and this may have an indirect impact on citizens' opinion and attitudes. [17]

[13] The project was supported by the Fundamental Rights and Citizenship Program of the European Commission.
[14] http://www.broad-project.eu
[15] This is the trilingual PET Portal & Blog, http://pet-portal.eu
[16] The professional videos are registered under Creative Commons license and can be freely downloaded from http://pet-portal.eu/video
[17] This is supported by the findings of researchers, for example Collins and Stahl (2002) or Shaw (2003), who have studied the moral considerations, intra-organizational relations and self-reported attitudes of IT professionals.

(2) The survey and the interviews will result in significantly different findings ("threshold of abstraction"). [18]

(3) [At least in Hungary] the majority of IT professionals are socialized to serve the stronger party (their principals or the information monopolies); however there exists a small but characteristic "freedom-minded" minority in the IT sector the members of which have different views. [19]

In working out the detailed plans for the online survey, we stated some further hypotheses (Leenes et al. 2010) , with special regard to the findings of earlier surveys:

- There are differences between distinct groups in the sample with regard to their knowledge of the Data Protection Act (DPA).
- Participants who find the DPA relatively more important also have more knowledge of it.
- There are differences between distinct groups in the sample with regard to their concerns about privacy protection.
- Privacy concerns reflect in people's actual online behaviour and work.
- There is a difference between Dutch and Hungarian respondents with regard to organizational consensus, defined as the overlap between an individual's attitudes about personal data and the attitudes about personal data held in the organization he/she is working in.
- There are differences between distinct groups in the sample with regard to hierarchy in the organization.
- There are differences between distinct groups in the sample with regard to their familiarity with and use of PETs.
- There are differences between distinct groups in the sample with regard to their degree of responsibility, defined as their resistance to carry out decisions about personal data if they disagree with them.
- Responsibility, defined as an individual's resistance to carry out decisions about personal data if he/she disagrees with them, is related to ratings of importance of DPA rights and concerns about privacy protection.
- There are differences in behaviour based on the differences in perceived behavioural control.

Leenes et al. (2010) also worked out a model to explain the interconnections between attitudes, external factors and behaviours, which is an extended model of Ajzen's theory of planned behaviour (1991). [20]

[18] This hypothesis rests on a certain realization, termed by the author as the „threshold of abstraction", whereby the answers depend not only on the severity of the breech of privacy, but also on the degree of abstraction, otherwise the level of palpability, associated with the violation. Typical survey questions dispense with most of the details, which means that they appear far more abstract than the problems outlined in an interview. A similar phenomenon emerged from the GPD survey (Székely 2010).

[19] We have advanced this hypothesis on the basis of the author's decades-long work as an expert and lecturer.

[20] We must point out here that the BROAD project, similarly to any research projects using interviews and surveys, has been designed to measure self-reported behaviour, rather than actual actions. Therefore, researchers under such circumstances need a hypothesis, which establishes the connection between the observable and the inferred elements, namely the knowledge, the attitudes and the actual acts – in this regard

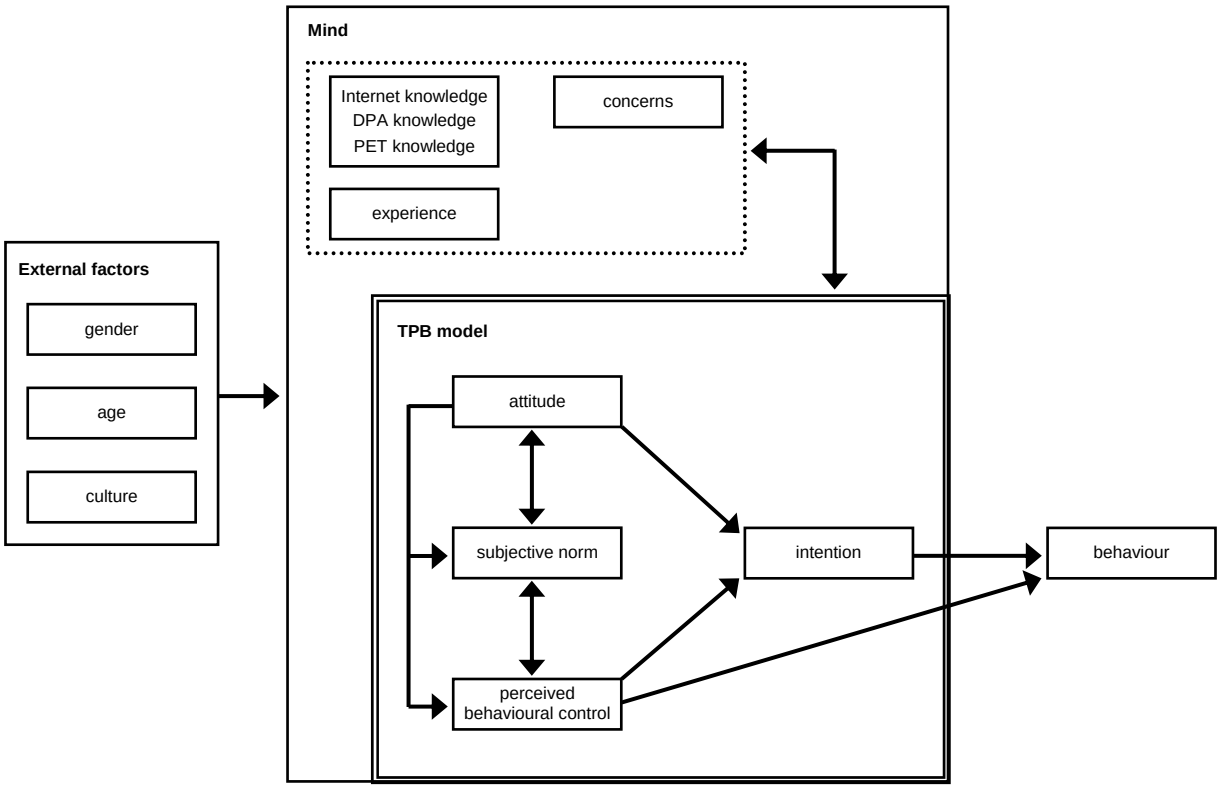

Fig. 1. Ajzen's extended model by Leenes et al. (2010)

The BROAD project covered numerous viewpoints, not only at the level of hypotheses and theoretical models, but also in the area of empirical research; the research report in itself could fill a smaller book.21 The present paper primarily concentrates on those elements of the research conclusions, which are relevant from the aspect of IT professionals' views on surveillance, as well as those, which could be of interest from the viewpoint of IT professionals' moral decisions and behaviours.

5. Methodology

Twelve, roughly one-hour-long semi-structured interviews were conducted in each country, using non-random samples. In The Netherlands we selected the respondents with the snowball method; the main objective here was to learn the views of people who occupied different positions within the same organizational hierarchy, with a special focus on the study of organizational consensus. In Hungary, the primary aim in selecting the respondents was to ensure that all the relevant groups to be covered in the subsequent survey would also be represented by a typical or characteristic member in the interviews. Since the author knew many of the selected respondents personally, the interviews were conducted by a colleague

we have borrowed the conclusions of Shaw's research, and also adjusted the general Fishbein-Ajzen model to our own research environment.

[21] At the moment, the manuscript forms part of the closing report of the BROAD project.

who was unknown to the interviewees, thus trying to reduce the risk of the respondents' echoing the views of the author.

We prepared an online survey for the qualitative study. Putting together a sample of IT professionals to be interviewed was not an easy task. Since representativeness of the unknown population was a methodological requirement, the sample population was put together in two stages: in the first stage we approached the selected professional groups, relying on the technique of distributing organization-specific tokens22 (controlled sample); and in the second, we announced the survey on public platforms and the respondents filled out the questionnaire in a form of self-assessment (random sample).

For the quantitative survey we compiled an online questionnaire, making use of the lessons learned from the interviews. The questionnaire contained 48 questions or blocks of questions, which incidentally turned out to be too many, as many of the respondents lost patience halfway through or lacked the necessary time, which resulted in a number of incompletely filled out questionnaires. The 48 questions were divided into 8 clusters:

A. Current work situation (1 question)
B. You and the organization you work for (5 questions)
C. General description of your work (3 questions)
D. Recent project (15 questions)
E. You and your personal experience with IT (4 questions)
F. Data Protection (10 questions)
G. General attitudes towards the Information Society (6 questions)
H Demographics (4 questions)

In carrying out the online survey, we relied on the software Limesurvey23. Only the active IT professionals were asked to fill out the complete list of questions; IT students and respondents belonging to the category "miscellaneous" (for example, retired IT professionals) automatically skipped clusters B through D, as they had no work environment.

A total of 1799 respondents filled out the questionnaire in the two countries. There were a large number of incompletely filled out questionnaires, which nevertheless yielded useful information in relation to certain questions. We could not, however, consider questionnaires, on which the respondents spent no more than two minutes. The resulting sample contained 1076 questionnaires for evaluation, which formed the basis of the analysis. The analysis was carried out using the programme IBM PASSWstatistics 17.

Promotional work in preparation for the survey proved less successful in The Netherlands than in Hungary; as a result, 77.9 % of the analyzed sample came from Hungary, and only 22.1 % from The Netherlands, which somewhat restricted the validity of the comparative conclusions between the two countries.

[22] These tokens make the categorization of the anonym responses from the various organizations possible; they also allow a comparison of the replies from the individual organizations.
[23] http://www.limesurvey.org

6. The interviews

In the following we shall focus on a number of specific findings emerging from the analysis of the interviews, with special emphasis on the topic of surveillance, which has been added to the subject-matter of the research project as a result of the Hungarian team's marked interest.

The twenty-four respondents represented a broad spectrum of IT applications and job titles. Interestingly, the majority of the respondents, who represent twenty-four IT application areas and came from an age bracket as wide as 27-72, consider themselves IT professionals, despite the fact that most of them have never received any formal education in information technology. Most of them have completed some training course in IT related subjects or acquired their professional skills in a self-taught manner. The older respondents obtained degrees in electrical engineering or mathematics, which can be considered the predecessors of the IT subjects.

> "Nowadays just about anybody with a little knowledge about computers can be described as an IT expert, but personally I would continue to insist on linking it to a college degree, as a minimum condition." [Information security expert, HU]

The interviews have revealed that the knowledge of IT professionals on personal data and data protection is equally sketchy in both countries. None of the respondents could provide either a formal or a substantive definition of personal data. Most of them gave a vague, general description, such as "data relating to a person", or mentioned examples of personal data, such as a credit card number. The respondents had similarly hazy notions of data protection. Most of them understood data protection as having to do with data security, although the Dutch respondents proved more critical in this regard. However, even data security proves secondary in the course of their work:

> "In the end functionality will also win over security, otherwise your systems are locked up and of no use." [ICT project manager, NL]

The respondents in both countries were also uninformed about data protection laws, with the majority believing that these had no relevance to their work.

> "I don't know the data protection law in any great details, but perhaps I know something about its effects, and also what it is about. It does not affect my work." [CEO IT association, HU]

> "I have a gut feeling about what can be done and what can't. This is more an ethical norm than a legal one" [innovator, NL]

Talking about the principles of data protection, one of the Dutch respondents made the following remark:

> "I have heard about them, but I cannot name them. It is a feeling in my head. I do however believe that I take these principles into account in my daily work" [developer, NL]

Another regrettable yet unsurprising finding emerging from the survey is that the active IT professionals also have insufficient knowledge and application experience in the area of PETs:

> "We do not really use PETs. There is no demand for them" [Unit manager, NL]

> "Not directly. This is the responsibility of the client" [consultant, NL]

> "Clients may eventually ask for them, but we have not heard of requests to insert PETs into our technology" [business development manager, NL]

6.1 Internet surveillance

Most of the (Hungarian) respondents had no objections to the surveillance of their Internet habits and behaviour; they felt that they "had nothing to hide".

> "But personally, I do not consider anything about my life to be out of the ordinary... If there is anybody out there who wants to observe me, then he might as well observe all the ten million inhabitants of this country. If I can be a target, so can anybody else." [marketing and sales manager, HU]

> "In any case, 98 or 99 percent of the people have nothing to worry, simply because no one cares what they are doing. And as for the remaining one or two percent, they must get used to the fact that this is how the world operates right now. " [Chief executive, IT security SME, HU]

Some of them distinguished between surveillance and the various grades of behavioural targeting, for example:

> "The simple fact that [a robot] watches my Internet habits and clicking patterns and complies a statistics about the pages I visit, effectively treating me as a number, this does not bother me too much. But if someone tied my name to the types of web pages I visit and found me on that basis with a business proposition, say, or if this information came up in the course of a job interview, for example, now that would be troubling. That would truly be troubling." [database expert, HU]

6.2 Workplace surveillance

Contrary to their views on Internet surveillance, the respondents were rather critical about workplace surveillance. While they considered some forms of workplace monitoring to be permissible, or even necessary, in general they showed solidarity with the employees. This can partly be explained by the fact that the majority of the respondents themselves worked, or used to work, in subordinate positions.

> "If the employees complete the task that has been assigned to them, they should be allowed to make phone calls or play on the computer a little." [head SW development firm, HU]

> "I am firmly against it. Let's face it, when somebody sits in front of the computer eight hours a day, and does nothing but works and works and works, that's not a good thing. And when this person wants to take ten minutes off to check something out on the Internet, people should not make a big fuss about this." [Web services manager, HU]

When it came to a workplace environment, the respondents took a much more nuanced view of the legitimacy of surveillance than with regard to the Internet, as the quote below can faithfully illustrate:

> "I hate these methods. Even the mere thought of me monitoring on my central computer terminal how [her secretary] in another office room is spending her time, gives me the creeps. [But] I would reprimand those civil servants who leak material, for example, out of political motivation." [CEO IT association, HU]

6.3 Surveillance by the State

The majority of the respondents have considered surveillance by the state both natural and acceptable. The same chief executive of an IT association, who regarded the monitoring of her secretary's work unacceptable, considers surveillance by the state natural:

> "Obviously, the state needs certain types of information, and it can compile the various databases any time it thinks necessary. There is nothing we can do about that." [CEO IT association, HU]

Although it concerns a public utility company, rather than the state, the rather excessive view below is educational:

> "Hungary has the strictest privacy protection regime in the world, one that verges on the irrational. … I mean that this not right that the BKV (Budapest Transport Company) should not be able to install surveillance cameras on its buses, in order to

monitor its passengers! ... We are protecting the criminals against the victims..." [university professor, HU]

6.4 Responsibility

An analysis of the interviews reveals that the majority of the respondents think that they bear no responsibility in ensuring the legality of the system they help to develop or run: the responsibility lies with either the management or the clients, but in any case outside their competency. We provide a few typical comments:

"This is not my area. The responsibility for complying with the law in this respect lies with the management. I do not know enough about it." [ICT innovator, NL]

"– *Besides calling the clients' attention to the legal consequences, is there anything else that you can do or want to do?*
– No, there isn't, but then again, this is not our job. I think that by doing this we have done all that is expected from us in the matter." [CEO, IT security SME, HU]

"Hungarian companies, and especially the smaller ones, don't give a damn about the whole thing." [CEO IT security SME, HU]

Personal, ethical considerations are most likely to pop up in interviews with the Dutch respondents:

"I have a gut feeling about what can be done and what can't. This is more an ethical norm than a legal one ... The main objective for me is to teach the students [and] their teachers how to learn ICT responsibly." [ICT innovator, NL]

In the case of a respondent from The Netherlands, the attitude is manifested in the ethical behaviour, at least in a self-reported manner:

"If a client would want to use the products we advise to target the IT behaviour of individual employees I would not accept the job." [business development manager, NL]

7. Survey data

The BROAD survey contains 48 questions and more than three hundred variables; even a summary review of their multivariate analysis would considerably exceed the scope of the present paper. On this occasion we have selected three groups of questions: making decisions about the handling of personal data and the compositions of views influencing such decisions in the organizational environment of IT professionals; the respondents' assessment regarding the protection of their information privacy; and the respondents' general ideas about the manifest features of information society.

7.1 Decision-making within the organization

Three-quarters of the active IT professionals declared that during projects that involved the handling of personal data there were explicit discussion about the specific ways of managing personal data. Nationality, age and the size of the organization were no factors in relation to the actuality of the discussions. The only difference seems to be that the colleagues directly responsible for implementing the IT methods are more willing to conduct internal discussions about the handling of personal data than the leaders of the organization.

The majority of the respondents agree with the decisions made about the handling of personal data throughout the project. Almost all of them claimed that if they happened to disagree with a decision, they would definitely let it be known. However, three-quarters of them said they would go along with the decision, even if they disagreed with it, with only twenty-five percent stating that in such a situation they would refuse to implement the decision. With regard to the handling of personal data, we tagged members of the first group as highly responsible, while members of the second group were termed as less responsible.

A detailed analysis of the data has revealed that neither nationality nor age appeared to be a factor with regard to responsible behaviour. The only significant difference in the composition of the two groups was related to position within the organizational hierarchy: Managers and IT architects had a higher representation in the group of high responsibility than IT engineers and IT testers. However, it is far from self-evident whether the results really reflected the differences of responsible behaviour or merely testified to the fact that people in higher positions were in a better position to refuse to carry out decisions they disagreed with.

In order to identify the underlying values that influence the decisions about the handling of personal data within the organization, we asked the respondents to rank the following items on a scale of one to five, from ‘completely irrelevant’ to ‘very important’:

(1) freedom of information
(2) security of data
(3) protection of personal data
(4) risk management
(5) cost effectiveness

Respondents rated security of data and the protection of personal data as the most important, followed by risk management, freedom of information and cost effectiveness; however, the differences recorded on the five-point scale were insufficient for a precise assessment of the importance of the various items. Using principal component analysis, it was possible to show that two factors played a significant role in the composition of the answers: one factor incorporated freedom of information, security of data and protection of personal data (we termed this the security & data protection factor), and the other was a combination of risk management and cost effectiveness (the risk management factor).

A study of the respondents' opinions about the views of their bosses, subordinates and professional peers in connection with the ranking of the above items has revealed that the security & data protection factor weighed little in their assessment of their colleagues. In other words, the respondents felt that they rated these values higher than their colleagues did.[24] At the same time, with regard to risk management and cost effectiveness, they apparently believed that these mattered more to them, than they did to their subordinates, but they still mattered less than their bosses and clients seemed to think. This opinion was independent of their position, their age, the size of their organization and their national identity.

A difference in the general attitude of the two national groups has been measured in that, in comparison to their Hungarian colleagues, the Dutch IT professionals attached greater importance to the extent their peer group valued the security & data protection factor, and also that the managers – irrespective of nationality – assessed the importance these items had in the eyes of their clients significantly higher than their colleagues employed as IT engineers did.

Organizational consensus refers to the degree to which an individual's attitudes coincide with the general attitudes within an organization. In our case we studied this consensus in relation to the importance attached to the assessment of the above values. An analysis of our data has revealed that neither age nor gender affected the organizational consensus. What did affect it, however, was nationality: according to their own assessment, the Dutch respondents were more in agreement with their colleagues than their Hungarian counterparts seemed to be. This conclusion, therefore, failed to support our general hypothesis, whereby the IT professionals in Hungary are more likely to identify with the views and value system of their bosses than those of their colleagues who have been socialized in established democracies.

7.2 Perceived behaviour regarding one's own privacy protection

According to the evidence of the face-to-face interviews, the majority of the IT professionals believe that IT professionals can protect their information privacy better than others. So we posed the following question to the survey's respondents: How closely do you agree with the suggestion that IT professionals can protect themselves in the Internet environment? Half of the respondents were convinced that they could adequately defend themselves on the Internet, while one-quarter definitely disagreed; the rest could not answer.

We also examined whether those who thought that they could protect themselves on the Internet made use of PETs in their own practice more than the rest of the respondents. We reached the conclusion that there was no significant difference in the use of PETs between members of this group and the others. Furthermore, we studied whether those who thought they could adequately protect themselves on the Internet actually used more PETs in the IT applications created or supervised by themselves than the others did. Here, too, we found

[24] In all probability the fact that people tend to judge their own attitudes more positively than their colleagues' has a lot to do with this finding. Since the questionnarie and the general topic of the survey convey the importance of the topic, the respondents are probably inclined to see themselves more interested and responsible in this area than they see their colleagues.

that there was no significant correlation between subjective assessment and workplace behaviour.

7.3 General attitudes towards the information society

We inquired about the respondents' level of concern for the following issues of apparent social significance:

- the quality of health services
- national security/terrorism
- the standard of education
- the (mis)use of personal data
- environmental issues
- unemployment
- immigrants and asylum seekers
- discrimination and equality
- limitation to the freedom of speech
- the emergence of a surveillance society

Of the listed items, the quality of health services, the standard of education, and the (mis)use of personal data received the highest scores.

Next we asked our respondents to indicate on a five-point scale – from Strongly disagree to Strongly agree – the extent of their agreement with the following statements in relation to privacy and the handling of personal data:

- People have lost control of the way their personal data is being collected
- New technologies provide a better privacy protection
- Privacy used to be better protected
- The protection of privacy has increased in the last couple of years
- The protection of privacy has decreased over the last couple of years
- Ordinary internet users do not know how to protect their data on the internet
- Privacy can be traded in against benefits
- Government and organizations collect personal data to gain control over people
- The protection of privacy undermines national safety
- IT professionals know how to defend themselves on the internet
- There is too much hype about the handling of personal information
- The modern world is the end of privacy, you must live with it
- People are not interested at all in what happens to their data
- Internet users are themselves responsible for the way their data is handled on the internet

Our principal component analysis has revealed the presence of five factors, which we marked with the terms 'changes', 'hype', 'lost control', 'disinterest' and 'own responsibility'.

According to the evidence of our analysis, the respondents agreed that the average Internet users had no idea how to protect themselves on the Internet and were not too bothered about the issue ('disinterest'). The respondents also concurred with the view that people lost control over the handling of their personal data and the government and the various organizations were collecting personal data in order to increase their influence over people ('lost control').

At the same time, it should be noted that one-third of the respondents could not decide whether they were concerned with the content of the listed statements; this indicates a considerable lack of interest for the handling of personal data.

In another list of items, we asked the respondents how big a role the following values played in their everyday lives:

- Freedom of information
- Security
- Protection of personal data
- Risk management
- Personal freedom
- Democracy
- Trust between people and government
- Trust between organizations and their customers
- Social order
- Cost effectiveness

The majority of the respondents rated all the listed items as valuable, without showing significant variations. In the detailed analysis we relied on the distribution of answers to select three factors, which we marked with the terms 'democracy', 'cost effectiveness' and 'security'. Of these three items, the values comprising the factor 'democracy' received the highest score, albeit with a small margin.

Finally, we checked whether the answers to the items list can be correlated and found that the answers to the following four items – each incorporated in a different question – show significant correlation: concerns about the misuse of personal data, concerns about the emergence of a surveillance society, concerns about people having lost control of the way their personal data is being collected, and concerns about a decrease of privacy in the last couple of years. Using these four questions, we created a new variable, which we termed 'privacy concern'.

We have concluded that significant variations exist in the respective views of the groups of respondents from three different aspects: nationality, student status and age. Respondents in The Netherlands were significantly more concerned about privacy than the Hungarian respondents were. Additionally, IT professionals were more concerned about privacy than IT students. Respondents between 35 and 49 years old were significantly more concerned about privacy than younger participants. At the same time, age, gender, the size of the organization and work position did not play any role in the level of privacy concern.

We also compared the level of privacy concern with various elements of self-reported behaviour. We found that the level of privacy concern was not related to the fact whether people used pseudonyms in their online activities, while there was a positive correlation between the level of privacy concern and people's – habitual or occasional – tendency to provide false personal information on the Internet.

8. Lessons learned – and things to do

Within the framework of the BROAD project, we have studied the views of people representing a profession generally regarded as influenced by the global technical development in two different social and cultural environments. In numerous cases, nationality proved irrelevant to both the final conclusions and the quantitative cataloguing of the answers; in other cases, however, it revealed significant differences. Therefore, some of our conclusions can be regarded quite general, while others emphasize the importance of the social and cultural differences between the two environments.

Foremost among our general conclusions is the recognition that IT professionals play a pivotal role in the implementation of projects that involve the handling of personal data, and that they possess great potentials to foster the rights and opportunities of the data subjects, a circumstance they themselves seem to be keenly aware of. IT professionals, regardless of age, gender and organizational background, had the same level of concern for data protection rights in both countries. They also held similar, rather pessimistic views about the knowledge and skills of Internet users in the area of personal data protection. However, when it came to the protection of their own privacy, they claimed to be more cautious than the rest, with half of the respondents thinking that they were capable of protecting themselves on the Internet.

The respondents from both countries shared a willingness to voice their concerns in case decisions irreconcilable with their views on the handling of personal data were discussed in their presence. However, the majority of the respondents in both countries admitted that in spite of such a disagreement they would carry out any final decisions.

In the areas of data protection and PETs, the Dutch IT professionals have shown themselves more knowledgeable than their Hungarian counterparts; they are also more concerned with the effects on the private sphere; and there is a wider agreement among them in professional matters.

It can be concluded that the attitudes of the IT professionals only marginally influence their actual behaviour, at least in the areas covered by the study. Those who care more about privacy do not appear to be using more PETs in their own online activities or in the products they have helped developing. On some occasions, such as workplace discussions, they appear to be more active.

As for our general hypothesis, whereby the IT professionals who design, build or operate the systems that manage personal data have a crucial role in the way these systems handle the personal data of the people concerned, this is fully in line with our collected data. As for the assumption that on certain issues the interviews and the survey yield substantially different information, this will need further clarification in the course of the detailed analysis.

Our analysis regarding organizational consensus has failed to support our original hypothesis, whereby IT professionals – at least in Hungary – tend to identify with the value system of their bosses or clients; here, however, further investigation would be necessary, before we can settle the issue.

One of our detailed hypotheses, whereby there are differences between distinct groups in the sample with regard to their concerns about privacy protection, has partially been borne out by our data: the Dutch and the older IT professionals are significantly more concerned with the protection of privacy than the rest. Our other hypothesis, whereby privacy concerns reflect in people's actual online behaviour and work, proved correct only to a limited extent, as the attitudes only marginally effect people's behaviour, according to our data. Our research results supported our expectations regarding national differences in organizational consensus.

Our hypothesis claiming that there are differences between distinct groups in the sample with regard to their degree of responsibility, defined as their resistance to carry out decisions about personal data if they disagree with them has essentially been unsupported by our data; the level of responsibility, which we have defined as someone not carrying out any decision that goes against his or her views on the handling of personal data, has turned out to be equally low in all groups.

But before we turn to drawing our final conclusions, we ought to run through the limitations of our research. One such limitation results from the specific nature of the sample: using qualitative methods, we have investigated a sample population of interviewees selected either by us or by their own colleagues, and we studied another, semi-controlled sample using quantitative methods. Several factors distorted our sample: it was possible that only those filled out our online questionnaire, who had attached great importance to the topic from the start, or only those who wished to conform to certain expectations, emanating either from the heads of their organization or from their teachers. The demographical composition of the survey sample was also uneven, and on the basis of the lessons learned from the analysis of the responses, certain modifications in some of the questions ought to be considered for any subsequent surveys. Finally, another limitation was the fact that only a few, indirect comparative analyses could be carried out because of the pioneering nature of the research.

*

After all, what do IT professionals think about surveillance? The emerging picture is rather complex, and for the time being we only see the details. The one thing that seems clear is that we can describe the role of IT professionals as neither "outright positive" nor "outright negative"; as a whole, they stand neither "for" nor "against" surveillance. What seems perfectly obvious, however, is that if we want to control or limit the emergence of surveillance society, especially in the Internet environment, then the only viable strategy must include the inculcation of IT professionals, or at least a large part of them, so as to encourage them to develop their knowledge and change their attitudes – and we need to do this not in a didactic way, but by taking into account their existing interests.

The results of one research project will not suffice to achieve this; we need educational programs, professional platforms and civil initiatives, as well as a meaningful dialogue between IT professionals and the other stakeholders in society. Naturally, we also need further research projects, either by repeating the BROAD survey in other countries or by improving its methods. In the interest of furthering this goal, the research consortium has decided to make available its raw data for all researchers interested in the topic.

References

Clark, M. Wesley. 2009. Pole cameras and surreptitious surveillance. *The FBI Law Enforcement Bulletin,* November 2009. http://findarticles.com/p/articles/mi_m2194/is_11_78/ai_n42126009/

Collins, Dervla and Bernd Carsten Stahl. 2002. The Importance of Codes of Conduct for Irish IS/IT Professionals' Practice of Employee Surveillance. In *The Transformation of Organisations in the Information Age: Social and Ethical Implications,* ed. Isabel Alvarez et al., 67–82. Proceedings of ETHICOMP 2002, Lisbon, Portugal.

Cyber-Ark Software. Annual "Trust, Security and Passwords" surveys 2007–2010. http://www.cyber-ark.com/constants/white-papers.asp

Dyzenhaus David, Sophia Reibetanz Moreau, Arthur Ripstein. 2007. *Law and Morality: readings in legal philosophy.* Buffalo: University of Toronto Press.

Electronic Privacy Information Center (EPIC). 2005. Public Opinion on Privacy.

Fishbein, Martin and Icek Ajzen. 1975. *Belief, attitude, intention, and behavior: An introduction to theory and research.* Reading, MA: Addison-Wesley.

Enright, Henry. The Winning Partnership: Law Enforcement & Video Surveillance Systems. The McMorrow Corporate Facilities Management Report. http://mcmorrowreport.com/articles/lawenforce.asp

Figliola, Patricia Moloney. 2007. Digital Surveillance: The Communications Assistance for Law Enforcement Act. CRS Report for Congress. http://www.fas.org/sgp/crs/intel/RL30677.pdf

Fishbein, Martin and Icek Ajzen. 1975. *Belief, attitude, intention, and behavior: An introduction to theory and research.* Reading, MA: Addison-Wesley.

Hanna, Michael J and Ronald P. Mattioli. 1995. Tactical surveillance with a twist. *The FBI Law Enforcement Bulletin,* August, 1995. http://findarticles.com/p/articles/mi_m2194/is_n8_v64/ai_17482629/

Harris Interactive. 2001. Privacy on & off the Internet: what consumers want. Technical Report, November 2001. New York: Harris Interactive, Inc.

International PET Portal and Blog. http://pet/portal.eu

Jones, Thomas M. 1991. Ethical decision making by individuals in organizations: an issue-contingent model. *The Academy of Management Review 16* (2): 366–395.

Kumaraguru, Ponnurangam and Lorrie Faith Cranor. 2005. Privacy indexes: a survey of Westin's studies. Pittsburgh, PA: Institute for Software Research International, School of Computer Science, Carnegie Mellon University. http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf

Leenes, Ronald and Isabelle Oomen. 2009. The role of citizens: what can Dutch, Flemish and English students teach us about privacy? In *Reinventing data protection?* ed. Serge Gutwirth et al., 293–316. Springer Science+Business Media B.V.

Lessig, Lawrence. 2000. *Code and other laws of cyberspace.* New York: Basic Books.

Oomen, Isabelle and Ronald Leenes. 2008. Privacy risk perceptions and privacy protection strategies. In *Policies and research in identity management,* ed. Elisabeth de Leuw, Simone Fischer-Hübner, Jimmy Tseng and John Borking, 121–138. Boston: Springer.

Shaw, Thomas R. 2003. The Moral Intensity of Privacy: An Empirical Study of Webmasters' Attitudes. *Journal of Business Ethics 46:* 301–318.

Székely, Iván. 2010. Changing attitudes in a changing society? Information privacy in Hungary 1989–2006. In *Surveillance, Privacy and the globalization of personal information. International comparisons,* ed. Elia Zureik et al., 150–170. Montreal & Kingston, London, Ithaca: McGill-Queen's University Press.

Zureik, Elia, Linda Harling Stalker, Emily Smith, David Lyon, and Yolande E. Chan (eds.). 2010. *Surveillance, privacy and the globalization of personal information. International comparisons.* Montreal & Kingston, London, Ithaca: McGill-Queen's University Press.