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

Author: Klitou, Demetrius
Title: Privacy-invading technologies : safeguarding privacy, liberty & security in the 21st century
Date: 2012-12-14
8.1 THE NEW THREATS TO PRIVACY

Today, when it comes to privacy issues, there is just too much talk about digital services and social networking websites, such as Facebook, and perhaps not enough attention paid to the potential impending reality that both clothes and walls could be rendered obsolete in terms of protecting privacy, thoughts could potentially be read, DNA analysis could become even more extensive and widespread, the deployment of UAVs could be routine for domestic surveillance, every object or person could be identified and tracked, and every activity out in public could be potentially recorded. Already, body scanners have been deployed at airports around the world, location tracking is commonplace and the advanced surveillance capabilities of CCTV cameras are widespread.

The methods and means of privacy invasion and mass surveillance have never been greater, as the threat to privacy, at present, is often directly relative to the existence and deployment of PITs. On top of that, the threat to privacy and liberty, posed by the latest PITs, are radical, unique and new, and are an affront to all domains and spheres of privacy. For instance, never before has technology been able to potentially see through clothes, read people’s minds, track every movement or automatically analyze and possibly predict human behavior.

These new threats to privacy are real and here, and are not hypothetical or potential. Body scanners are rapidly being deployed, enhancements to CCTV cameras are increasingly being carried out and the scope and capabilities of RFID and GPS applications is evermore advancing. While HIMs have not yet reached a critical mass, given the circumstances, there is arguably real potential for their significantly greater (or perhaps widespread) deployment to occur within the next 10 years.

The threats to privacy from PITs are not homogenous and the threats can emanate for different reasons and from different causes. For instance, the threats can come from

---

Indeed, however, the threats to privacy posed by Facebook (and other social networking websites) should not be overlooked and are increasingly becoming worrisome.
the abuse or misuse of the privacy-intrusive capabilities of technologies (i.e. when users of PITs intentionally or unintentionally violate privacy and/or data protection laws), or simply from the technology itself regardless of how it is used, or from the intended or unintended purposes of the technology. Moreover, not all the threats can be predicted and these uncertainties are in themselves a threat and equally should not be ignored (Sollie and Düwell, 2009).

The increasing development, deployment and use of body scanners, HIMs, and CCTV microphones and loudspeakers, not to mention the many other PITs in existence or in development, are changing, where applicable, the level of privacy we enjoy over our physical bodies and the nature of our public space. With the advancement of the latest PITs, the risks, threat level and temptation of abuse have drastically increased. The means of privacy invasion and mass surveillance have never been greater and the threats to privacy and liberty posed by the latest PITs are uniquely new.

However, that does not mean that any or all of the PITs addressed should be completely banned. That would require a complex explanation and methodology of determining what technologies should be considered acceptable and unacceptable based on a comprehensive ethical framework on evaluating technology.\(^{823}\)

On the contrary, these technologies should arguably be embraced, as long as the adequate legal framework is in place. Although PITs pose serious threats to privacy, they offer in return a common good, i.e. potential benefits in terms of security, convenience, electronic commerce and, in the case of RFID implants, also improved and safer healthcare delivery. Nevertheless, while benefits exist, the threats and risks persist.

8.2 BEYOND PRIVACY AND DATA PROTECTION

If left unchecked and without the adequate legal framework in place, the latest PITs threaten not just the right to privacy, but other individual civil liberties as well. The latest PITs pose a threat to other civil liberties by causing a ‘chilling’ effect on fundamental rights, such as the freedom of speech, freedom of association and freedom of movement – freedoms, which are necessary in a free and democratic modern state. This is particularly true for technologies capable of mass public surveillance.\(^{824}\) For instance, the intrusive

\(^{823}\) For further discussion, see Sollie, Paul and Marcus Düwell (eds), Evaluating New Technologies: Methodological Problems For The Ethical Assessment Of Technology Developments (Springer, 2009).

\(^{824}\) For further discussion, see the Memorandum by Victoria Williams for the House of Lords Constitution Committee inquiry into the impact of surveillance and data collection upon the privacy of citizens, available at: http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/8051402.htm
capabilities of HIMs could have a ‘chilling’ effect on the freedom of movement, as people become more cautious where they travel. HIMs, or the RFID microchips in travel cards for that matter, could also be used to interfere with the freedom of movement by denying or ‘digitally cutting-off’ a person’s access to mass public transportation. The capability of CCTV microphones, if left unchecked, could potentially have a ‘chilling’ effect both on the freedom of expression out in public and the freedom of assembly, and, thus, could also frustrate the right to protest peacefully. CCTV loudspeakers could especially have a detrimental effect on personal autonomy and dignity.

Besides, the right to privacy and data protection laws are not always enough to defend liberty or check every threat posed by the latest PITs. In the US, the freedom from unreasonable search, embodied in the Fourth Amendment of the US Constitution, serves as the basis of the reasonable expectation of privacy. But, this expectation is subjective and vulnerable to the constantly advancing development and deployment of PITs. Moreover, even though location information can potentially reveal sensitive personal information, the location information generated by RFID and GPS applications is not necessarily or adequately afforded the protections of the Fourth Amendment, due to the current ambiguous division of what is private and what is public, and the lack of a legal recognition of privacy out in public.

In the EU and the UK, data protection laws were formulated, for the most part, to control personal data, which is conventionally understood to mean information that relates to identified or identifiable individuals. But, this formulation also certainly has its downsides. For instance, even though the images produced by (fully-intrusive) body scanners are seriously privacy-invasive, the images may not necessarily always constitute personal data or data in personally identifiable form per se, since a person arguably cannot be identified from the images alone, and therefore data protection laws alone may not be applicable or sufficient for regulating body scanners. While the recording of general sound out in public by CCTV microphones is intrusive, it is also arguably not considered personal data per se and, therefore, is not covered by data protection laws in the UK (since it is not focused on any particular individual, in accordance with UK case law). Data protection laws also do not apply to CCTV loudspeakers, since the loudspeakers are not used to process personal data, but CCTV loudspeakers, nonetheless, may pose a threat to the right to be left alone. Likewise, even when the use of RFID
microchips is not initially linked specifically to identified individuals, threats to privacy still remain, since the data could potentially later be used, nonetheless, to identify, track and profile individuals. This brings us to the next downside. Data protection laws do not apply to anonymized data. However, with advanced data mining techniques and group profiling (i.e. the categorization of people), the effects could be just as bad as (or even worse than) processing personal data. Moreover, while the Data Protection Directive (Directive 95/46/EC) is certainly applicable for transactional acts, the Directive may not cover adequately non-transactional acts, such as interactions/relationships and opinions.

Applying the principles of privacy/data protection alone, therefore, cannot entirely address the potential impacts and threats of public surveillance technologies. As Victoria Williams equally reminds us, in order to assess the impact of public surveillance schemes, the consideration of the effects on personal autonomy is required, concluding that lawmakers must also assess how the observation of public places creates a risk of ‘chilling’ the right to exercise the freedom of speech and assembly. Accordingly, the right to privacy and other civil liberties or human rights need to be protected in an integrated manner. The legal framework should, as a result, not only focus on the right to privacy and data protection, but rather also emphasize on safeguarding other fundamental rights, where applicable, and better extending the regulation of privacy infringement into other domains, such as the human body and the public sphere. Hence, the legal and technical solutions for addressing the intrusive capabilities of PITs must not only be concerned with the right to privacy, but should also take into consideration, where applicable, other civil liberties and social and moral issues simultaneously.

8.3 DEFICIENCIES OF THE EXISTING LEGAL FRAMEWORKS

The legal framework in the US, as it stands now, is unequipped, for the most part, to meaningfully counteract the privacy threats posed by body scanners and HIMs, while the UK legal framework is equally inadequate to regulate CCTV microphones and CCTV loudspeakers. In terms of fulfilling the principles of privacy, with regards to these latest technologies, the deficiencies and dilemmas of the US and UK legal frame-

---

825 For that reason, the Article 29 Working Party specifically addresses this issue and argues that the scope of Directive 95/46/EC applies to targeted profiling/online behavioral advertising. see Article 29 Data Protection Working Party, WP 171, Opinion 2/2010 on online behavioural advertising, 22 June 2010.

826 see supra note 824.
works are evident. As deducted from the case studies, the deficiencies of the current legal framework, pertaining to privacy/data protection in the US and the UK/EU, are partly due to the fact that traditional policy or legal-based solutions focus predominantly on data controllers/processors, service providers and operators/users of PITs, as opposed to their developers/manufacturers. This approach fails to address the privacy-intrusiveness of the technologies concerned at the design stage.

While there are certainly significant deficiencies in the US and UK legal frameworks, with regards to the latest PITs, neither legal framework necessarily requires a complete overhaul. Instead, the legal frameworks require both amendments to existing laws, and new laws based on what continues to remain valid.

Moreover, while some might argue that the privacy principles are losing validity, particularly in light of the latest technologies and the impending ubiquitous information society; this is only true if we let this occur. As demonstrated through the case studies, the common principles of privacy protection can still form the foundation to work from, and there is no need to reinvent the wheel at this juncture. The current principles of privacy indeed remain as the basis of assessing the adequacy of a legal framework in terms of protecting privacy and continue to be relevant and valid both for formulating new legislation and designing for privacy. However, this does not mean that there is no need whatsoever now or in the future to revisit the privacy principles, where necessary, or to even establish and add new principles.827

Nevertheless, what is most essential is that there are adequate means, mechanisms and methodologies for enforcing and implementing the existing privacy principles against the evermore advancement of technology. Although both the US and UK/EU legal framework express the goals and elements of privacy protection, the practical rules on how to realize them are inadequate. Without adequate and specific rules in practice, the developers of body scanners, HIMs and CCTV microphones and loudspeakers, for example, are left to voluntarily determine their own way of realizing these goals, and thus their level of responsibility for doing so or lack thereof.

Indeed, there is a vacuum of law, which must be dealt with accordingly, in order to bring the law up to speed with the latest threats to privacy and other civil liberties posed by the latest technologies. Throughout this dissertation, the recommendations on dealing with the deficiencies of the US and UK legal frameworks primarily focused on both legislative/policy and technological solutions, based on the widely established fundamental principles of privacy, as opposed to overhauling or reversing the problem-

827 Indeed, the OECD Secretariat supports a “global privacy dialogue” that is intended to revisit the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. See the DHS Privacy Office Annual Report to Congress, July 2007-July 2008, p. 77.
atic, altering (and potentially somewhat outdated) analysis and interpretation of courts within the US and UK.

While there is, to a certain extent, already a legal basis for PBD within the US and UK/EU legal frameworks (see section 9.6), the prevailing deficiency concerns the fact that the relevant provisions are primarily only applicable directly to data controllers and service providers, as opposed to the designers and/or manufacturers of the PITs themselves. Data protection/privacy laws and regulations have all too often focused on requiring data controllers/processors to comply. Unfortunately, even the draft proposal for an EU General Data Protection Regulation, while indeed a step in the right direction, proposes data protection by design (i.e. PBD) requirements that are erroneously only applicable to data controllers.

Although the laws could have an indirect effect on manufacturers, whereby the data controllers in turn compel or put pressure on manufacturers, this has evidently proved insufficient. Instead, the law should specifically emphasize additional obligations on the manufacturers/developers.

Part II evaluated/assessed the adequacy of the legal frameworks in the US and the UK and proposed some of the necessary amendments to enhance these legal frameworks, in order to ensure that the right to privacy is preserved, in light of the intrusive capabilities of the four particular PITs addressed. In addition to the proposed legal solutions, a number of technical and/or design solutions were proposed for each PIT. Technical and design solutions for the sake of protecting privacy are collectively known as “privacy by design”. The next chapter (Chapter 9) outlines what is specifically meant by “privacy by design”.

828 see Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft.

829 Ibid., Article 23.