Face Recognition and Privacy enhancing techniques[1]

Alberto Cammozzo

Abstract. *This paper aims to clarify "face recognition" privacy issues emerging in social networks and public places. Reviewing current uses, a taxonomy of face recognition technologies is suggested to discern what aspects of face recognition impact the most on privacy, what are the main issues, and what privacy enhancing techniques are currently available to address them. Findings underline the need for a privacy-by-design approach where social computing follows evolving social norms without puncturing social context integrity.*

1 Introduction

Applications of the data analysis techniques called *automatic face recognition, facial recognition* or *face processing* have recently raised many concerns when used in social networks, especially Facebook, and in public places, in particular for face-in-the-crowd surveillance applications. Most of these technologies have been developed to monitor high security areas but over time face recognition has silently migrated in other segments of the security market (surveillance, attending systems), in some consumer products (games, cameras) and in online services and social networks. This has fuelled the debate on social acceptability of facial biometric technologies: someone considers them "creepy", others asks for their regulation, while someone considers face recognition an innovation that naturally belongs to our future world. This paper examines the privacy issues raised by the multiple uses of face recognition in social computing. Section 2 summarizes and exemplifies the different biometric techniques that commonly go under the name *face recognition.* Besides the elements of a typical face recognition system from the engineering point of view, uses in social networks suggest a specific taxonomy. Section 3 connects the main privacy issues with privacy literature and the concept of *contextual integrity* [Nissenbaum, 2004]. Section 4 briefly exemplifies some ways to tackle face recognition intrusiveness, either by architectural choices or by opt-out techniques designed by users. Conclusions suggest the adoption of a privacy-by-design and transparent approach where computer code follows social norms.

2 Face recognition techniques and use

Face processing comprises a number of technologies applied to digital still pictures or video streams, each with very different impact on privacy and social life. Some of them may raise

1 Presented at Ethicomp 2011, Sheffield Hallam University, 14-16 September 2011.
Published in the conference proceedings as: Alberto, Cammozzo. "Face Recognition and Privacy enhancing techniques." In *The Social Impact of Social Computing*, edited by Andy Bissett, Terry Ward Bynum, Ann Light, Angela Lauener, and Simon Rogerson, 101--109. Shaffield Hallam University, Sheffield, UK: Sheffield University, 2011.

serious privacy issues, while some other may be useful to protect people's privacy.
In order to develop a clear debate on their uses, a match between common sense terms and engineering ones has to be attempted.
Systems engineering literature usually describes the main tasks performed by a generic full-featured face recognition biometric system as follows:

> The **match** task evaluates to what extent the biometric **signatures** extracted from the unknown face exemplar(s) and the biometric signature(s) stored during the **enrollment** stage as reference **template**(s) are similar. The match score has to be compared against some a priori defined **threshold** value. Matching takes place against a single template (for **verification**), or against a list of candidate templates (for **identification**). Verification is also referred to as **authentication** [Wechsler, 2007, p. 4].

This formal task breakdown is conceived for biometric identification purposes. The three essential tasks are: (1) the *enrolment* of a person, that builds a one-to-one relation between a single face template and a single name; (2) *identification,* that matches a face against the template database and returns only one identity (or "user unknown") in a one-to-many relation; (3) *verification,* that matches a face with a claimed identity and returns "true/false" in a one-to-one match [Li and Wechsler, 2005; Wayman, 1997].

In a different way, the common sense meaning of "face recognition" that emerges in the ongoing privacy debate describes many different technologies, some of which do not easily fit in the theoretical framework outlined above.
The main tasks of face recognition systems used in social computing can be described as follows: face *detection* helps isolating faces in some image; face *matching* achieves a *partial enrolment*, extracting face features and generating a template, often without linking it with any name; then face *matching* allows to group together faces that match the same signature; *identity association* links a a full identity to a face template and finalizes a partial enrolment, and at last identity *verification*, that fits to the engineering description of biometric authentication systems.

(1) ***Face detection*** is used to automatically detect or isolate faces from the rest of the picture and –for videos– track a given face or person in the flow of video frames. These algorithms only spot a face in a photo or video and do not extract signatures nor enrol people. Their complexity and performance may vary if the environment surrounding the face is controlled or uncontrolled in terms of lighting, distance, location, number of individuals [Weng and Swets, 2002, p. 66]. Detection can to some extent discriminate age, sex and even emotional cues, leading to possible application in *intentions* recognition [Tistarelli and Grosso, 2010]. Recent smartphones and digital cameras embed face detection, often complemented with smile detection. In fact, the terms "face recognition" are used improperly for face detection: the device does no enrolment, identification nor verification, nonetheless detection is a prerequisite for these tasks.
Face detection can play a great role in protecting privacy: Google Street View automatically blurs faces of passers-by [Google, 2011a] as does Microsoft Streetside [Microsoft, 2011]. Human rights activist application for smartphones SecureSmartCam [Nunez, 2011] does automatic obfuscation and encryption on photos: this feature is designed to protect the identity of protesters in public events and gives witnesses the freedom to take pictures

without the risk of compromising the protesters in case phone is lost, confiscated or stolen. However, the false sense of assurance this technology gives, may rise privacy concerns in case of errors (false negatives): pictures may be publicly released under the false assumption all faces are blurred, and this may lead to consequences for people depicted.
Face detection is increasingly used is in *digital signage*, the name for those digital out-of-home (DOOH) video billboards located in streets, stores and stations. These devices often include a video camera and displays targeted ads appropriate to the age, sex and mood of people watching. Those devices raise privacy concerns [Geiger, 2009] especially when they covertly *store* face signatures in order to recognize returning visitors and engage interaction with them (in a "Minority report" style experience). However *storing* face features crosses the line between face detection and face matching systems (see below). While many digital signage companies publicly state they don't store visitors data, market pressure steers in that direction [QBR, 2011].

(2) ***Face matching*** automatically compares a given face with archived ones and selects those images where the same person is present. A template has to be created extracting features from every single face, so that a matching algorithm compares each new signature against all templates: highest scores match the most resembling faces, arguably from the same person. It's important to notice that there is no need to know the target's personal identity to generate a reference template and these can be collected without any identity attached. When used on video streams, matching allows tracking of people movements. The ability to detect a face in non-optimal conditions, like a video stream from crowded places is called "face in the crowd" problem [Wechsler, 2007, p. 121]. It is often used by surveillance services in courthouses, hotels, stadiums, malls, train stations or airports, sometimes combined with long range iris scan or other biometrics. Application of these systems are appearing daily in newspapers [PraguePost, 2011; Prensa, 2011; Whitehead, 2011] and market press releases [Prnewswire, 2011].

The technical possibility of performing face matching on the wealth of publicly available pictures stored in social computing sites raises many privacy issues, the most concerning being the construction of a *facial search engine*. A face-search engine could perform an "upload face and search matching faces" service or even expose Application Program Interfaces (APIs) allowing for a "search by face signature" service. While in the first case searcher has to provide a face image, to look for matching faces, in the second case searcher has only to provide an autonomously calculated face signature. Interoperable face signature generation standards (see below) will push further in that direction.
Google announced to have developed a face recognition search engine [Milian, 2011], but decided not to deploy it for privacy concerns [Warman, 2011].

It may be useful to attempt a further classification of face matching activities applied to social computing. Depending on who keeps the stored pictures and who performs the signature matching, face matching can be performed in a *joint* or *disjoint* form. In *joint store/match,* who keeps the pictures also performs the matching. In *disjoint store/match,* a third party downloads pictures stored in social networking sites, generates signatures and either keeps a copy of pictures along with their signatures, or keeps only URL/signatures pairs, discarding pictures.
A very relevant variable is also *scope:* how wide is the "search space" made available to face match searches? Access can be restricted to pictures uploaded by the user who performs the

search, or be unrestricted, so that the searcher can access the whole wealth of pictures available in the repository. Social networks often add additional intermediary restrictions (friends, groups). Another relevant variable is who triggers, or *initiates,* face signature generation. Enrolment can be initiated *on user demand* on selected pictures, or *by default* on any picture uploaded, independently of users intentions. If signature generation is run by default, target may never be informed of being enrolled.

On the one hand *joint* store/match is suitable for social networking operators that offer face matching as a value-added service to their own customers, as happens both with Google's Picasa Web album face-matching, intended for home photo organization [Google, 2011b] and Facebook's tag suggestions [Mitchell, 2011]. Even if with different default settings, both run face-signature generation *by default*, without asking consent to user, who has only the opportunity to ignore the tag suggestion or opt-out from service.
On the other hand, *disjoint* store/match is offered by a third party who complements storage services that don't provide face recognition. Alternatively, such a service may be offered to users who want face matching on pictures encompassing multiple storages, each accessible with different credentials. For instance I can run face matching on all the pictures I have stored under my Facebook, Flick and Picasa accounts running an application provided by a third party. This is precisely what Viewdle's Social Camera [Viewdle, 2011] does: it matches faces in smartphone snapshots with images in Facebook and Flickr, allowing users to upload and tag photos. A similar service, limited to on Facebook accounts, is run by Face.com [Face.com, 2011]. Another possible use of a disjoint store/match face matching service is a global face search engine. It could be directed to general public use, like the one dismissed by Google, or be oriented to private customers, like governments and private organizations interested in background checks and security clearances.

Summarizing all possible combinations of *joint/disjoint* activities, *scope* and *initiative* and excluding non viable solutions we have five possible face matching scenarios (see Table 1 below). Signature generation can be done:

(a) by storage provider, by default, on any picture uploaded by any user, without access restriction to search service. So far no service of this kind has been announced;
(b) by storage provider, by default, on any picture uploaded, limiting search access only to pictures available from the user's account. This is what Facebook recently did, and Google Picasa Web albums does since 2009;
(c) by storage provider, on user demand, generating signatures only on selected pictures from those available with users credentials. So far no service of this kind has been announced among the major social computing platforms;
(d) by a third party (nor the user nor the storage provider) on all publicly available pictures. This is what Google internally developed but did not release, due to privacy concerns;
(e) by a third party, only on pictures available on storage providers, and accessed through user's credentials. Services of this kind have been demonstrated as prototype or are currently offered.

It is quite surprising that the most privacy-respectful option, the one allowing a user to *run* face matching only on specified picture sets, has not been adopted by any social computing platform.

store and match ***activities***	**matching faces access** ***scope***	**face signature generation** ***initiative***	Examples
joint	unrestricted access to storage provider data	by default	*none known so far*
	restricted to user data	by default	*Facebook tag suggestion, Google Picasa face matching*
	restricted to user data	initiated by user	*none known so far*
disjoint	unrestricted access to publicly available data	initiated by third party	*Google (unreleased)*
	restricted by user's credentials	initiated by user	*Face.com photo tagger, Viewdle Social Camera, Astonishing Tribe Recognizr (unreleased)*

Table 1: Taxonomy and examples of face matching technologies

(3) ***Identity association*** consists in linking personal data to a reference face template already generated by a partial enrolment procedure. Any signature matching the reference template can then be linked to data disclosing personal identity.
There are many differences between access control applications of face recognition and social network use of the same technologies. In an ideal context and in absence of errors, only one identity is allowed for a given template, so that a person will always be linked to an unique template. This is not (yet) the case in social networks.
Among the many classifications of biometric applications, literature considers enrolment as *overt* or *covert*, *cooperative* or *non-cooperative*. If the user *is aware that a biometric identifier is being measured, the use is overt. If unaware, the use is covert* [Wayman, 1997]. A system is cooperative if a deceptive user cooperates with the system *to appear to be someone she is not, or attempting not to cooperate to not appear to be someone known* [Wayman, 2002].
In most biometric systems used for access control, enrolment is cooperative and overt, and template generation happens at the same time identity is provided (and often supported by other credentials). On the contrary, for most surveillance and "face in the crowd" applications, identity association never happens, the aim of surveillance being chiefly *identity verification*: verifying the presence of unauthorized/unwanted persons.

In social networks, as we have seen, a partial enrolment can take place by default before (if ever) a full identity is made available: templates are generated before they are assigned to a given identity (if ever). Identity association takes place as a second phase, often through *tagging*. Tagging can be done by the target user himself (cooperatively) or by someone else. Moreover, tagging can be done with full real name, partial real name (i.e. first name), pseudonyms (as a user-name) or even with false identities. This may lead to multiple tags (identities) for a single template. Even so, the abundance of personal information provided by users and their friends in social networks may disclose much more information than a real

name.
Once one or more tags are *manually* associated to a template, any face matching with that template can be *automatically* tagged in the same way. This is what happens with *tag suggestions* offered by Facebook and others. Even if the *decision* to accept or reject the the tag-template association is left to the user, suggestion remains as an hint to a possible identity association. Depending on social network policies and defaults, targets may be informed or not that they have been associated with an identity and may or may not be able object to the identification.

(4) ***Face identification or verification*** is an automated operation that allows to check if a face signature matches or not against a single template (*verification*) or a list of candidate templates (*identification*).
Use of face recognition for identity verification is spreading: even recent operating systems allow biometric authentication instead of using traditional user-name/password credentials. Main recent applications are devoted to *access control* and *time attendance* systems in firms, schools [Donnelly, 2011], and even hospitals looking for missing patients [Stelter, 2011]. Face recognition often complements other biometric techniques as *iris scan* or *fingerprints* in national *border processing*, *immigration* and government and *police* applications such as suspects check or search for documents issued to people giving false identities. Casinos, hotels and malls use face recognition for security purposes, to verify that their customers are not in lists of known trouble gamblers or shoplifters. A kids-only social network [WhatsWhat, 2011] is using webcam face verification to authenticate children and grant them access.
When these face recognition solutions rely on face templates stored in a proprietary form, then systems are closed and not interoperable: signatures from one system cannot be matched with templates from another vendor. But interoperable and standard signatures would boost the effectiveness of face recognition: for this reason standards are developed and maintained for data interchange, testing and API definition. For instance, section 5 of ISO/IEC standard 19794 is dedicated to Face Image Data [Wechsler, 2007, p. 56].
While standardization makes interoperability easy, it makes easier also to abuse of data that leaks out of the system.
The presence of interoperable face matching systems applied to the wealth of pictures present in social networks is frankly scaring. The implementation of *disjoint* store/match systems where surveillance, attendance, security and monitoring systems are able to access to social computing platforms outlines an identification system distributed on a global scale. The technical *possibility of ubiquitous identification and surveillance of all citizens virtually anywhere in the world—and by anyone,* for someone is already existent [Rosen, 2011]. This scenario has been described since 1999 by Phil Agre [in Gruteser and Grunwald, 2004] and named “Privacy Chernobyl”. It is likely that a “privacy panic” reaction would spread with the emergence of ubiquitous and globally interoperable surveillance, with people signing-off social networks, pulling pictures off the net or enacting obfuscation techniques (see below).

3 Privacy Issues

The major privacy issues outlined above can be summarized as follows:

(1) **Unintended use**: data collected for some purpose and in a given scope is used for some other purpose in a different scope, for instance surveillance cameras in malls used for marketing purposes, photos sent along a CV used by a potential employer for a pictorial background check, and so on. This has been widely referred to in literature as *unauthorized*

secondary use [Smith, Milberg, and Burke, 1996] and leads to *function creep* [Woodward, 1997]. In addition, biometric templates can also be stolen due to poor data protection and security, and leak outside the system along with identity information, boosting identity theft [Tillmann, 2009].

(2) **Data retention**: the period templates are stored should be appropriate for the purpose they are collected. Expired information should be deleted. Information beside the declared purpose of the system should be discarded. Privacy respectful digital signage systems should not enrol users, and time attendance systems should delete templates of users that are no more authorized. A correctly designed problem gambler detection systems in casinos does not keep templates of non-problems customers [Canton, 2011]. Otherwise, the famous quote from New Yorker's Cartoon in 1993 "On the Internet, nobody knows you're a dog" should be changed in "On the Internet, nobody *forgets* you're a dog".

(3) **Context leakage**: images taken in some social context of life (affective, family, workplace, in public) should not leak outside that domain, breaking what has been called the *contextual integrity* of our socio-technical systems:

> A central tenet of contextual integrity is that there are no arenas of life not governed by norms of information flow, no information or spheres of life for which "anything goes." Almost everything—things that we do, events that occur, transactions that take place—happens in a context not only of place but of politics, convention, and cultural expectation [Nissenbaum, 2004].

According to Nissenbaum, the two main sets of norms dealing with privacy are *norms of appropriateness* that *dictate what information about persons is appropriate, or fitting, to reveal in a particular context*, and those that *govern flow or distribution of information—movement, or transfer of information from one party to another or others.* As a consequence, *common practices are understood to reflect norms of appropriateness and flow, and breaches of these norms are held to be violations of privacy* [Nissenbaum, 2004].
To avoid puncturing privacy contexts, systems should comply to social norms. Computer code should follow social code, and not the opposite. New technologies should not push too far innovations on personal information availability and flow until appropriate norms for the preservation of contextual integrity are in place. Otherwise a demand for explicit regulation through *legal* code will arise [Lessig, 1998].
Following this principle, images taken in public places or public events should never be matched with those from other, closed contexts without explicit consent, since the public social context assumes near anonymity (nobody wears a name tag in public). This is especially true for sensitive data, like pictures taken in political or religious public gatherings, but should also apply to other images released for specific purposes in a specific privacy context.
Since people are different and have different privacy preferences, these *should become part of the "privacy" context* of computer programs for social networks [Sheng, Yu, and Dustdar, 2010, p. 403] that should embed the flexibility of social norms.

(4) **information asymmetry**: pictorial data may be used without explicit consent of the person depicted, or even without the knowledge that that information has been collected for some purpose. It has been pointed out that new surveillance technologies differ from

traditional ones in that the controller has access to information about the controlled that the controlled himself ignores [Pagallo, 2008, p. 209]. I may have no hint that there are pictures of me taken in public places and uploaded in repositories; as long as pictures have no identity associated my privacy is still quite preserved, but as soon as face matching is applied, privacy contexts are challenged, and with identity association, they are definitely torn. Someone may easily collect and hold information about me I do not know myself. Non transparent disjoint face recognition systems that parse anonymous pictures in public repositories and match them with identified faces may collect information the targeted person will never now. This is particularly concerning in case of false positive errors, where a picture of someone else (possibly depicted in some act I disapprove) may be covertly associated with my identity, and someone could possibly take some decision about me based on some erroneous information I ignore.
Last but not least, governments have enough power to access information stored in social computing companies under their jurisdiction. If an image repository performs default enrolment and matching on uploaded pictures, it holds information that may be used for forensic purposes. As a consequence, uploaded images could be used to identify people. This is what happened in Vancouver, where images taken in recent riots are used to identify rioters [Hui, 2011]. As already noted [Brey, 2004], false positives and the *problem of error* may have extremely serious consequences in these uses.

4 Privacy enhancing techniques

Since many agree that face recognition is here to stay, what do we need to preserve privacy? A privacy by design approach [Cavoukian, 2009] takes into account privacy issues from the beginning. In face recognition systems, a number of solutions have been devised: one possible approach is splitting the matching and identification tasks, using strong cryptography to *hide the biometric data as well as the authentication result from the server that performs the matching,* allowing real-time identification from a surveillance camera only of a given person, without compromising the privacy of others [Erkin et al., 2009]. Another work introduces a de-identifying algorithm that makes identification ineffective while preserving most facial details in the pictures. This technique is appropriate to preserve opt-out choices and is achieved through an image alteration that introduces loss of specific information [Newton, Sweeney, and Malin, 2005]. One promising technique [Boult, 2006] tries to *ally the privacy concerns while supporting security goals* through encryption of biometric tokens (such as face template). This hides the user's identity and allows the revocation of tokens without interfering with the matching capability, that takes place in encoded form. This privacy-preserving transform may *enhance* system accuracy, as do other “Untraceable Biometrics” [Cavoukian and Stoianov, 2009].
Users have spontaneously developed devices to protect their privacy in public places. Face recognition opt-out techniques include wearing a pixelated hood [Backes, 2010] or special face recognition camouflage make-up [Harvey, 2010] and even temporary blinding CCTV cameras [Where is My Data, 2008]. The creation of *pixelated fashion* (including eye-wear) is perhaps a hint that privacy sensitiveness is migrating into common sense [Designboom, 2011]. The TagMeNot project invites to wear or display a specific QR-code that links to the project's site, where the will of not being tagged and recognized is clearly stated, so it could not be ignored [Cammozzo, 2010].
Obfuscation technique aims at re-balancing the information asymmetry, producing misleading, false, or ambiguous data [Brunton and Nissenbaum, 2011]. Uploading and tagging faces with wrong names (or the opposite, wrong faces) produces a misleading

identity association and may have a positive effect in protecting real data.

5 Conclusions

With privacy in mind, after comparing the tasks defined by biometric face recognition research to the activities taking place in social computing environments, a taxonomy has been suggested to help future debates. The main components are face detection, face matching, identity association and identity verification. Face matching poses the greatest concerns when associated with social networks. Current face recognition services have been classified in a matrix comprising joint/disjoint store and match operations, scope and signature generation initiative (user initiated or by default). Two of the combinations are left unused: the one that is most respectful of privacy and the most invasive one (a global unrestricted matching service). Privacy issues have been categorized in four main classes: unintended use, data retention, context leakage, and information asymmetry generation. Computer codes that define social network architecture should follow social norms, not stretch them and tear contextual integrity. Creative solutions devised by users to opt-out from face recognition in public places reveals a genuine need for privacy. Face recognition can be used respecting privacy, provided privacy-by-design approaches are adopted.

References

Backes, M., (2010, December 23), Pixelhead, online at http://www.martinbackes.com/new-artwork-pixelhead/ accessed 21.6.2011

Boult, T., (2006), Robust Distance Measures for Face-Recognition Supporting Revocable Biometric Tokens, IEEE International Conference on Automatic Face and Gesture Recognition (Vol. 0, pp. 560-566), Los Alamitos, CA, USA: IEEE Computer Society, doi:http://doi.ieeecomputersociety.org/10.1109/FGR.2006.94

Brey, P., (2004), Ethical Aspects of Face Recognition Systems in Public Places, Journal of Information, Communication & Ethics in Society, 2(2), 97-109,

Brunton, F., and Nissenbaum, H., (2011, May 2), Vernacular resistance to data collection and analysis: A political theory of obfuscation, First Monday, 16(5), online at http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3493/2955 accessed 2.5.2011

Cammozzo, A., (2010), TagMeNot privacy: no face recognition, don't tag, blur my face., online at http://tagmenot.info/ accessed 21.6.2011

Canton, D., (2011, June 20), Privacy by design initiative has merit, London Free Press, London, online at http://www.lfpress.com/money/columnists/david_canton/2011/06/17/18300361.html accessed 20.6.2011

Cavoukian, A., (2009), Privacy by design ... take the challenge, Toronto: Information and Privacy Commissioner of Ontario, online at http://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf accessed 24.6.2011

Cavoukian, A., and Stoianov, A., (2009), Biometric Encryption: The New Breed of Untraceable Biometrics, Biometrics: Theory, Methods, and Applications, 655-718, doi:10.1002/9780470522356.ch26

Designboom, (2011, June 5), pixelated fashion by Kunihiko Morinaga of Anrealage, online at http://www.designboom.com/weblog/cat/8/view/14507/anrealage-pixelated-fashion.html accessed 21.6.2011

Donnelly, K., (2011, May 9), End is in sight for roll calls as schools face the future - Latest News, Education - Independent.ie, online at http://www.independent.ie/education/latest-news/end-is-in-sight-for-roll-calls-as-schools-face-the-future-2641123.html accessed 20.6.2011

Erkin, Z., Franz, M., Guajardo, J., Katzenbeisser, S., Lagendijk, I., and Toft, T., (2009), Privacy-Preserving Face Recognition, In I. Goldberg & M. J. Atallah (Eds.), Privacy Enhancing Technologies (Vol. 5672, pp. 235-253), Berlin, Heidelberg: Springer Berlin Heidelberg, online at http://www.springerlink.com/content/wk623747g141r063/ accessed 2.5.2011

Face.com, (2011), face.com developers site » FAQ, online at http://developers.face.com/docs/faq/ accessed 19.6.2011
Geiger, H., (2009, September 10), Digital Signage and Consumer Privacy, www.DigitalSignageExpo.net, online at http://www.digitalsignageexpo.net/DNNArticleMaster/DNNArticleView/tabid/78/smid/1041/ArticleID/1826/Default.aspx accessed 14.6.2011
Google, (2011a), Privacy – Google Maps with Street View, online at http://maps.google.com/help/maps/streetview/privacy.html accessed 14.6.2011
Google, (2011b), Add name tags in Picasa - Picasa Help, online at http://picasa.google.com/support/bin/answer.py?answer=156272 accessed 18.6.2011
Gruteser, M., and Grunwald, D., (2004), A Methodological Assessment of Location Privacy Risks in Wireless Hotspot Networks, In D. Hutter, G. Müller, W. Stephan, & M. Ullmann (Eds.), Security in Pervasive Computing (Vol. 2802, pp. 10-24), Berlin, Heidelberg: Springer Berlin Heidelberg, online at http://www.springerlink.com/content/0h4kduy2fxypa3jc/ accessed 21.6.2011
Harvey, A., (2010), CV Dazzle by Adam Harvey, online at http://cvdazzle.com/ accessed 21.6.2011
Hui, S., (2011, June 17), ICBC offers facial-recognition technology to Vancouver police's riot investigation, Straight.com, Vancouver, online at http://www.straight.com/article-399779/vancouver/icbc-offers-facialrecognition-technology-vancouver-police%E2%80%99s-riot-investigation accessed 21.6.2011
Lessig, L., (1998), The Laws of Cyberspace, Net '98 conference, Presented at the Net '98 conference, Taipei, online at http://www.lessig.org/content/articles/works/laws_cyberspace.pdf accessed
Li, F., and Wechsler, H., (2005), Open Set Face Recognition Using Transduction, IEEE Transactions on Pattern Analysis and Machine Intelligence, 27(11), 1686-1697, doi:http://doi.ieeecomputersociety.org/10.1109/TPAMI.2005.224
Microsoft, (2011), StreetSide: Dynamic Street-Level Imagery via Bing Maps, online at http://www.microsoft.com/maps/streetside.aspx accessed 14.6.2011
Milian, M., (2011, March 31), Google making app that would identify people's faces - CNN.com, online at http://edition.cnn.com/2011/TECH/mobile/03/31/google.face/ accessed 19.6.2011
Mitchell, J., (2011), Making Photo Tagging Easier, The Facebook Blog, online at http://www.facebook.com/blog.php?post=467145887130 accessed 18.6.2011
Newton, E. M., Sweeney, L., and Malin, B., (2005), Preserving Privacy by De-Identifying Face Images, IEEE Transactions on Knowledge and Data Engineering, 17(2), 232-243, doi:http://doi.ieeecomputersociety.org/10.1109/TKDE.2005.32
Nissenbaum, H., (2004), Privacy as Contextual Integrity, Washington Law Review, 79, 119,
Nunez, B., (2011, March 9), The Secure Smart Camera App for Human Rights Video : Video For Change, online at http://blog.witness.org/2011/03/ssc accessed 14.6.2011
Pagallo, U., (2008), La tutela della privacy negli Stati Uniti d'America e in Europa, Giuffré,
PraguePost, (2011, April 20), Prague Transport (DPP) is to introduce face-recognition security cameras that will record the movements of every single passenger, Prague, online at http://www.praguepost.com/news/8380-monday-news-briefing.html accessed
Prensa, (2011, April 28), Panama will purchase facial recognition system from U.S., Prensa.com, Panama, online at http://mensual.prensa.com/mensual/contenido/2011/04/28/hoy/english/economy_7004.asp accessed 14.6.2011
Prnewswire, (2011, January 27), Regular Offenders Can be Identified by Facial Recognition Technology, online at http://www.prnewswire.co.uk/cgi/news/release?id=138606 accessed 14.6.2011
QBR, (2011, June 9), Yeahpoint unveils "future" of shopping - Industry News - Queensland Business Review, online at http://www.qbr.com.au/news/articleid/74162.aspx accessed 14.6.2011
Rosen, J., (2011), The Deciders: Facebook, Google, and the Future of Privacy and Free Speech, Governance Studies at Brookings, The Future of the Constitution, (12), online at http://www.brookings.edu/papers/2011/0502_free_speech_rosen.aspx accessed
Sheng, Q. Z., Yu, J., and Dustdar, S., (2010), Enabling Context-Aware Web Services: Methods, Architectures, and Technologies, CRC Press,
Smith, H. J., Milberg, S. J., and Burke, S. J., (1996), Information Privacy: Measuring Individuals' Concerns about Organizational Practices, MIS Quarterly, 20(2), 167-196, doi:10.2307/249477

Stelter, L., (2011, May 24), Major healthcare provider turns to analytics, Security Director News, online at http://www.securitydirectornews.com/?p=article&id=sd201105w4KUe accessed 20.6.2011

Tillmann, G., (2009, October 27), Opinion: Stolen fingers: The case against biometric identity theft protection - Computerworld, online at http://www.computerworld.com/s/article/9139965/Opinion_Stolen_fingers_The_case_against_biometric_identity_theft_protection accessed 24.6.2011

Tistarelli, M., and Grosso, E., (2010), Human Face Analysis: From Identity to Emotion and Intention Recognition, In A. Kumar & D. Zhang (Eds.), Ethics and Policy of Biometrics (Vol. 6005, pp. 76-88), Berlin, Heidelberg: Springer Berlin Heidelberg, online at http://www.springerlink.com/content/n7q76106t234778h/ accessed 14.6.2011

Viewdle, (2011), Android Augmented Reality + Face Recognition Mobile App - Viewdle SocialCamera®, online at http://viewdle.com/products/mobile/index.html accessed 18.6.2011

Warman, M., (2011, May 18), Google warns against facial recognition database, The Telegraph, online at http://www.telegraph.co.uk/technology/google/8522574/Google-warns-against-facial-recognition-database.html accessed 18.6.2011

Wayman, J. L., (1997), A generalized biometric identification system model, Conference Record of the Thirty-First Asilomar Conference on Signals, Systems & Computers, 1997 (Vol. 1, pp. 291-295 vol.1), Presented at the Conference Record of the Thirty-First Asilomar Conference on Signals, Systems & Computers, 1997, IEEE, doi:10.1109/ACSSC.1997.680201

Wayman, J. L., (2002), Technical Testing and Evaluation of Biometric Identification Devices, In A. K. Jain, R. Bolle, & S. Pankanti (Eds.), Biometrics (pp. 345-368), Boston, MA: Springer US, online at http://www.springerlink.com/content/p72u557k5437g1x5/ accessed 14.6.2011

Wechsler, H., (2007), Reliable face recognition methods: system design, implementation and evaluation, Springer,

Weng, J. J., and Swets, D. L., (2002), Face Recognition, Biometrics: personal identification in networked society, A. Jain, R. Bolle, and S. Pankati, Eds (pp. 65-82), Berlin: Springer,

WhatsWhat, (2011), What's What: Social Networking for Kids, online at https://www.whatswhat.me/ accessed 24.6.2011

Where is My Data, (2008, July 17), IR used to defeat CCTV, online at http://whereismydata.wordpress.com/2008/07/27/ir-used-to-defeat-cctv/ accessed 21.6.2011

Whitehead, T., (2011, March 2), Unmanned spy drones and facial recognition cameras could soon be the norm, The Telegraph, online at http://www.telegraph.co.uk/news/uknews/law-and-order/8355091/Unmanned-spy-drones-and-facial-recognition-cameras-could-soon-be-the-norm.html accessed 14.6.2011

Woodward, J. D., (1997), Biometrics: privacy's foe or privacy's friend?, Proceedings of the IEEE, 85(9), 1480-1492, doi:10.1109/5.628723