Facing Facism

unique biometric identifiers and data totalitarianism: socio-technical considerations

Alberto Cammozzo[1]

Abstract. *New technological facts, combined in a social perspective, highlight a possible data totalitarianism based on unique biometric identifiers. This article reviews those technological and social facts, highlights the socio-political implications and ventures some suggestion. Technological facts are: 1) non-cooperative visual biometrics, especially face and behavior recognition (gait), and their multimodal combination; 2) wearable computing and augmented reality; 3) face recognition search engines; 4) interoperable biometric systems, making easy to enroll and recognize targets on different independent systems, and 5) the build-up of massive biometric data collections. Those technological facts may combine in a socio-technical arrangement where a securitarian culture prevails, as highlighted by: 1) social networks that fight a war on pseudonymity; 2) the "right to surveillance" is socially and legally uncoded and asymmetrically distributed: ubiquitous surveillance is unevenly flanked by practices as crowdsourced surveillance or sousveillance. This socio-technical setup highlights a condition where a new form of data totalitarianism may raise, especially in countries where technological advancement is not combined with equal improvement in privacy-awareness and democracy. Besides data protection authorities rulings, what initiatives could help to face this threat on a socio-technical ground? 1) Reestablishing information symmetry. This could be achieved through publicly accessible face recognition search engines and the decoupling of identity provider and content repository services, allowing both real name requirement and pseudonymity; 2) protecting privacy in the public context, assuming default opt-out from identity recognition.*

Keywords: *privacy, biometric data, face recognition, gait recognition, wearable computing, interoperability, pseudonymity, identity providers, data breaches, surveillance, sousveillance, re-identification.*

1 New technological facts

There have been recent evolutions in face and gait recognition; new devices and services with

[1] 18 Mar 2013 – Cammozzo.com and TagMeNot.info
Submitted for presentation at ETHICOMP2013 conference, June 2013
http://www.sdu.dk/en/Om_SDU/Institutter_centre/Idk/ethicomp2013

potential severe effects on privacy are being tested.

1.1 Non-cooperative Visual Biometrics: face and behavior recognition

Visual biometric techniques rely on images or video footage. *Non-cooperative* biometric systems are effective even on targets wishing to defeat the system in one or more phases of the recognition process, while collaboration is required in *cooperative* recognition (Goudelis, Tefas, and Pitas 2010; Wayman et al. 2005, 9). The main phases of the process are: *enrollment* (the extraction of a personal biometric feature, template or signature from images), *verification* (matching of other images against a single template) and *identification* (matching against a list of candidate templates) (Wechsler 2007, 4). Examples of *intrusive* visual biometrics are fingerprints, retina, iris, vein and palm scans and optical skin reflectance; while *non-intrusive* or *non-collaborative* visual techniques are centered on face recognition on conventional images or on facial thermograms (depicting heat). Thermograms are independent from ambient illumination and best suitable for covert surveillance. Increasingly, personal behavior characteristics such as smile or gait are used. (Goudelis, Tefas, and Pitas 2010; Xuan Zou, Kittler, and Messer 2007). Examples of *non-visual* biometrics are, for instance, voice recognition, body odor or head resonance (Wayman et al. 2005, 3).

A recent application based on the intuition that «colors of clothes, decorations, and even human motion patterns, can together make up a "fingerprint"» was demonstrated in a wearable-computer setup, with Android Galaxy phones and camera-enabled glasses (Wang et al. 2013).

A so-called "multimodal" approach comprises the full range of technologies that could be used on a given image or video. An example is the FBI's Next Generation Identification searchable database that includes «facial imaging, scars, marks, and tattoos» and has «room to accommodate future biometric technologies (i.e., voice, gait, etc.) as they become available and prove reliable» (US Federal Bureau of Investigation 2009).

1.2 Wearable computing & Augmented reality

Google recently unveiled "project Glass" (Google 2013), a pair of glasses that "see" what is in the view field, overlaying information in a head-up display manner. This head mounted device could recognize voice commands, record video, take pictures, display text messages and maps. This kind of wearable computer "augments" the visual scene with additional information coming from the automatic analysis of the environment.

Even if visual biometric recognition does not seem to be in current Google glass features and was explicitly excluded from previous Google project Goggles (Adee 2010), it's well into its technical possibilities. Face recognition and gait analysis will eventually make its way into wearable computing devices. Probably Google Glass biometric recognition policy will be consistent and allow face recognition only for Google+ users that opted in. But third parties (like Baidu, see section 1.3, or Facebook) could develop apps with different privacy policies.

Governments already have such devices designed explicitly with biometric visual recognition in mind (Yapp 2011; Beckhusen 2013).

Privacy implications of this technology are substantial, since wearable computing devices similar to ordinary glasses conceal the fact that they are acquiring video footage and automatically analyzing the scene. Everybody in sight is a potential target of biometric recognition. People are unaware of having their biometric features being analyzed and potentially recorded and ignore what use will be done of this information.

Advocates of wearable computing affirm that making available to the masses a biometric recognition device could reestablish an information asymmetry and also help “democratizing surveillance” (Weber 2012) and develop “sousveillance” or “watchful vigilance from underneath” (Mann, Fung, and Lo 2006) (more on this in section 2.2).

For instance, a wearable face recognition device could help to spot “agents provocateurs” and prevent them to disturb peaceful manifestations, as theorized in (Marx 2013). In fact, during “Occupy” protest in New York, pictures taken by protesters were used to identify and sue an officer spraying pepper on demonstrators (Coscarelli 2011), even if no use of automatic face-recognition was reported.

As we will see in section 2.2, it would be inappropriate to consider Project Glass as “sousveillance”, given that all footage is centrally stored at Google's.

1.3 Face recognition search engines

Recently Baidu, the main Chinese search engine company, is testing an open face recognition search engine (识图 http://stu.baidu.com) (Ong 2013). This test service lets anyone upload an image containing a face and then run a search on matching images published anywhere on the Web. Google had decided in 2011 (Warman 2011) not to run a similar service because “too creepy”.

Face recognition search services seen so far restrict their results on the image set provided by their users (store and match operations are *joint)* on consensual targets (Cammozzo 2011). Baidu face search fills the gap, delivering a *disjoint* store and match service on any target, with an *unrestricted* access to publicly available data.

Even if it's in a testing phase and not very reliable, such a search engine is a genuine novelty and has many privacy consequences (Cammozzo 2012). On the one hand it may represent a “stalker's paradise”, on the other it may help anyone to figure out what kind of personal pictorial information is available and allow to take privacy measures. As we will see in section 2.2 it may help to fill an information asymmetry, also “democratizing surveillance” (Acquisti, Gross, and Stutzman 2011), and help to mature social norms that are more respectful for visual privacy.

1.4 Interoperable biometric systems

Data collected on one biometric recognition system can be used on another system only if the two are interoperable. This means that people enrolled on one type of software could be recognized by another system if those are interoperable and they share their data. For instance, US DHS and FBI biometric systems are interoperable (US Federal Bureau of Investigation 2012), while most of the apps that use face recognition to unlock a smart-phone are not.

Currently few systems are genuinely interoperable, probably because face recognition has been widely used only for the last few years and the technology needs to mature and consolidate; but as soon as this happens interoperability will soon emerge along with compliance to standards. For instance biometric passports already comply to ISO/IEC standard 19794 part 5 that defines biometric data interchange formats for face image data (ISO - International Organization for Standardization 2011). Compliance to standards and interoperability allow airport authorities to automatically match passengers faces with the biometric features and identities encoded on their passports: this is what “smart e-gates” do.

As already noted (Cammozzo 2011) while standardization and interoperability are technically desirable, they also make abuses easier in case of data breaches or leaks. Once interoperable biometric data for a given person is out of the system, any other system complying with the standard will be able to identify the target person.

1.5 Massive data collection, data breaches and government access

Even if its reliability is disputed, face recognition use is exploding. According to some analysts (Acuity 2009), biometric market will strike revenues of 10 billion dollars in 2017, of which up to 33% may come from face recognition. Visual biometric databases are being built around the world at an incredible pace for the most diverse reasons: from surveillance, to biometric passports, attendance systems, digital signage and marketing, down to games and authentication on cellphones. In the coming few years, it will be difficult for anyone to avoid being enrolled in some kind of visual biometric system.

In April 2011, the Sony PlayStation Network suffered a massive data breach: personal data of 77 million users were copied off the Sony servers. It's not known if biometric visual information was included in the personal and “profile data” that leaked; It may be possible, given that the PlayStation gaming system includes a face recognition system since 2009 (Flatley 2009).

What will be the consequences of massive visual biometric data breaches on a similar scale? If the biometric data is stored in interoperable format, the first consequence is that face and gait, more than names, will be a way to link data coming from different sources, even anonymous ones, legitimate or not. Moreover leaked data could be used to identify people in public spaces through CCTV surveillance, wearable devices or even your home smart video intercom.

Governments in all countries have ways to lawfully access any kind of personal information for law enforcing reasons. This applies also to social network data, independently of privacy options (see for instance Robinson 2012), and may happen in an automated way. Some countries may exert pressure even outside clear legislative frameworks. Depending on the democratic and legal status of a country, agreements between companies detaining biometric data and governments may be more or less transparent to the public and biometric data could be used for political purposes.

Goverment also hire private contractors to design and run CCTV and surveillance systems. Those contractors will likely serve private customers, and only a very strict privacy policy will keep companies off the temptation of sharing (or selling) data, or taking advantage of economies of scale. Suspects that this is already happening have hit the press (Wolf 2012).

2 Social facts

These technical facts make possible a global, unique, personal identifier around biometric face/gait recognition. This could be combined and linked to current social, economic and political trends to give an overall socio-technical perspective.

According to Nissenbaum, the two main sets of social 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 socially established privacy contexts, technological systems should try to comply to social norms. Computer code should follow social code, rather than assuming a “privacy is dead” attitude. On the other side, also social codes should adapt to accommodate technological innovations.

2.1 #nymwars: the war on pseudonymity and the identity market

The two biggest social networks, Google+ and Facebook, are fighting a war against their users pseudonymity. Their respective “real name requirement” pages state:

> Real Name Requirement for Google+: [...] it’s important to use your common name so that the people you want to connect with can find you […]. Name Changes are limited to 3 changes every 2 years. [...] Your nickname should represent you as an individual, and should not be used to represent a business or profession. (Google 2012a)
>
> Facebook is a community where people use their real identities. We require everyone to provide their real names, so you always know who you're connecting with. This helps keep our community safe. [...] The name you use should be your

> real name as it would be listed on your credit card, student ID, etc. [...] We require everyone to provide their real names, so you always know who you're connecting with. If you'd like to list a second name on your account (ex: maiden name, nickname, or professional name), you can add an alternate name. (Facebook 2013a)

Users not complying will see their accounts suspended. For suspended accounts, both companies are relying as a last resort, on some form of government-issued photo identification (Facebook 2013b; Google 2012b).

These measures have been heavily criticized under ethical and privacy considerations as a defense of corporate interests (Elliott 2012) and as an authoritarian exercise of power against vulnerable people and marginalized communities: those who use pseudonyms are not only pedophiles, but also rape survivors, victims of stalking, political and sexual minorities; or simply, communities with a tradition of nicks and pseudonyms, as artists and "techies" (Boyd 2011). Often pseudonyms are not a sign of "lack of integrity", but a security need and a way to preserve the norms of appropriateness and flow of a privacy context.

A strong reason for social networks to require real names is that they are silently fighting for a share in a new global single-sign-on market as identity service providers. Besides the business of providing social network services for their users and that of advertising, they are becoming identity service providers (so called "connect" services) for third parties, like other content providers who don't want do build a users database for authentication themselves (Ko et al. 2010): increasingly we see sites asking users to authenticate using Facebook or Google+ credentials.

As we will see below, from a security and privacy point of view it would be better to unbundle the two services: one party should acts as an identity provider and know nothing about the content, the other keeps sensitive biometric content, ignoring the real identity and trusting the identity provider.

Given the huge mass of biometric data stored in social networks, real name policy implies that pictures and videos linked with each unique real name identity could lead to re-identification, as it has already been demonstrated (Acquisti, Gross, and Stutzman 2011).

2.2 Securitarian culture and asymmetric "right to surveillance"

Our cities, malls, shops, schools, bars and even homes are increasingly pervaded with CCTVs and webcams, often for security reasons but also for marketing or even more frivolous purposes. But who is watching who is often not so clear. Classic "panoptic" surveillance enacted by government, communities and shop owners is being flanked by other practices: with the terms *crowdsourced surveillance* Schneier (2010) describes (mostly failed) examples of traditional centralized surveillance where the task of watching the actual video stream is crowsourced. In these examples, volunteer or paid citizens watch pictures and videos to spot shoplifters (interneteyes.co.uk) or the US-Mexico border (texasborderwatch.com) or people in no-mans lands (US HomeGuard). Another practice is what Steve Mann, a renowned researcher and advocate of wearable computing, calls s*ousveillance* or "watchful vigilance from underneath". Mann also foresees the emergence of a state of "*equiveillance*" or the balance between surveillance and sousveillance (Mann, Fung, and Lo 2006). This concept recalls the idea that dispersing visual recording technologies between citizens could help "democratizing surveillance" (Acquisti, Gross, and Stutzman 2011; Weber 2012).

We are being socialized into accepting video surveillance "for our own security", even if we know that often security cameras actually are not about security. While traditional surveillance is usually accepted socially and regulated by law, other processes –especially sousveillance– are socially and legally uncoded and not so clearly accepted. Mann reports that while he was in a Paris McDonalds he had been assaulted because of his wearable computing video recording device (Mann 2012). McDonalds employees asked him to stop filming to "protect the right of privacy of staff and customers". Mann observed that staff and customers were already filmed by McDonalds surveillance cameras, and later raised the question on his blog: «It would seem that society has come to accept ubiquitous surveillance without questioning it. Regardless of whether or not ubiquitous surveillance is justified, should those people who accept surveillance not also accept sousveillance?». This question stays open, along with others on the social consequences of ubiquitous visual equiveillance.

Another example is the "social experiment" run by the Seattle "Creepy Cameramen" who goes around holding a video-camera and recording people's reactions (Bishop 2012) and saying «I'm just taking a video» since «video cameras are everywhere...». Reactions go from people getting up and leaving, others insulting him, pushing him put of places, calling the police or physically attacking him.

What these examples show is an amazing social asymmetry: people have become rather indifferent to CCTV cameras in streets, offices, malls and even watching them from billboards, but are pretty reactive when someone actively films them. There is strong social resistance against being video-recorded by unknowns for unknown reasons. Sousveillance – except in some specific contexts – does not seem to be viable. I push forward the hypothesis that what people accept or refuse are the underlying *reasons* behind being surveilled, not surveillance *per se.* If there is the hint of a reason, and that reason is implicitly accepted under the assumption of an advantage or at least no harm, surveillance is tolerated.

3 Combined technical and social asymmetries

On the issue of visual biometrics, all four kinds of code interfere: the legal, the social, economic rules and computer programs (Lessig 1998; Lessig 1999).

On the technical side, we have seen that visual biometrics (face and gait recognition) can represent a unique personal identifier. We have also seen that an enormous mass of those identifiers are being collected from a number of operators, that if biometrics are standard or interoperable those identifiers can be linked to a single identity (re-identification), and that massive personal data breaches do indeed happen. This introduces a huge information asymmetry: unknown entities may know things about us that we don't know.

On the social side we have seen another asymmetry: while sousveillance is considered creepy, biometric recognition and ubiquitous surveillance are socially accepted, and social network companies are succeeding in enforcing a real name requirement against pseudonymity. This allows them to become identity providers for third parties, but also to link each single unique biometric identifier to a single real life identity. Legal codes and social norms accept and regulate top-down surveillance but are socially and legally unprepared to cope with bottom-up sousveillance.

This combination introduces another greater asymmetry: the ability to control the appropriateness and flow of information about us belongs to someone that is not us. According to the Nissenbaum definition, this means that our privacy is not in our hands. On a global scale, this ability is in the hands of few companies and governments. Because of technical innovations and social unpreparedness, societies face a possible data totalitarianism based on biometric unique identifiers that may be called “facism”.

Is the society aware? The imminent launch of Google Glass is producing harsh reactions (Champion 2013). The presence of surveillance glasses in streets and bars will perhaps represent a “privacy Chernobyl” event, as described since 1999 by Phil Agre (Gruteser and Grunwald 2004). A no-return event that raises a “privacy panic” reaction on the dangers of surveillance. This kind of reaction may actually deepen the asymmetry, as the victim of a panic reaction could be the right to sousveillance, and not the ruthless exploitation of personal data: a ban for people from to record in public with wearable devices, and not a ban on ubiquitous surveillance “for security reasons”.

4 How to face it? Reestablishing information symmetry

Data authorities have become quite responsive to issues linked to biometric visual data. US FTC has issued recommendations on face recognition (US Federal Trade Commission 2012) and in the EU a new data protection regulation has been proposed that explicitly takes into account “large scale biometric personal data” and the “right to be forgotten” . Besides the necessary legal initiatives, what are actions are likely to foster a social response in a direction that avoids data totalitarianism?

While computer programs behavior is to some extent predictable, it's extremely difficult to design measures that could impact on social norms. Some measures, playing on awareness and allowing systemic feedback, could perhaps help to reestablish an information symmetry.

1) Publicly accessible face recognition search engines, as the test site of Baidu, can help reestablish a symmetry. Anyone can check what biometric data is linkable to her identity, leading to a full awareness of what kind of visual information is available also to others. She can also take appropriate steps to delete data she wishes to stay private, provided an adequate “right to be forgotten” is enforceable. This reduces the risk that personal data is provided to thirds by entities running similar services covertly. One great downside of this approach is

that only privacy-aware and tech-savvy users will be able to limit the availability of personal biometric data.

2) To face the issue of biometric data linked to real identities, we could design and investigating a technical arrangement where the identity provider is separated from the content or service provider (eg. social networks, e-mail, website requiring authentication). The entity who identifies the user should know nothing about her content, while the party who provides or stores user content trusts the identity provider about her access credentials. This is what happens with single-sign-on systems. Each user could, if he wishes, use multiple identities from several different identity providers. While keeping the freedom to use pseudonyms for most services, users can be required to provide real names, according to the type of service requested. Reliably linking together multiple identities to one real name is made more difficult. Law enforcement could access both parties (identity and content) with a single warrant.

3) As a general rule, privacy in the public context should be protected assuming default opt-out from non-cooperative biometric visual recognition. Users enrolled in biometric recognition systems should be specifically informed on all possible uses, scope and duration of their data. Exceptions for specific cases should apply.

The matter is evolving very rapidly, so we are going to see in the next few years what will be the outcome of the interaction of computer code with social norms together with market and legal rules.

Acquisti, Alessandro, Ralph Gross, and Fred Stutzman. 2011. "Faces Of Facebook-Or, How The Largest Real ID Database In The World Came To Be." In *Blackhat 2011*. http://www.blackhat.com/html/bh-us-11/bh-us-11-archives.html#Acquisti.

Acuity. 2009. *The Future of Biometrics Market Research Report*. Acuity Market Intelligence. http://www.acuity-mi.com/FOB_Report.php.

Adee, Sally. 2010. "Google: 'Goggles Does NOT Do Face Recognition'." *IEEE Spectrum Blog*. http://spectrum.ieee.org/tech-talk/consumer-electronics/portable-devices/google-goggles-does-not-do-face-recognition.

Beckhusen, Robert. 2013. "Navy's Next-Gen Binoculars Will Recognize Your Face | Danger Room | Wired.com." *Danger Room*. 02. http://www.wired.com/dangerroom/2013/02/binocular-face-scan/.

Bishop, Todd. 2012. "'Creepy Cameraman' Pushes Limits of Public Surveillance — a Glimpse of the Future? - GeekWire." *GeekWire*. November 1. http://www.geekwire.com/2012/seattles-creepy-cameraman-pushes-limits-public-surveillance/.

Boyd, Danah. 2011. "'Real Names' Policies Are an Abuse of Power." *Apophenia*. http://www.zephoria.org/thoughts/archives/2011/08/04/real-names.html.

Cammozzo, Alberto. 2011. "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.

———. 2012. "Do We Need an Open Face Recognition Search Engine?" In Universidad Nacional del

Sur. Bahia Blanca. Argentina. http://sedici.unlp.edu.ar/handle/10915/23870?show=full.

Champion, Edward. 2013. "Thirty-Five Arguments Against Google Glass." *RELUCTANT HABITS*. http://www.edrants.com/thirty-five-arguments-against-google-glass/.

Coscarelli, Joe. 2011. "Anonymous Outs NYPD Officer Who Pepper-Sprayed Occupy Wall Street Protesters." *Nymag.com*, September 26. http://nymag.com/daily/intelligencer/2011/09/anonymous_outs_nypd_officer_wh.html.

Elliott, Deni. 2012. "The Real Name Requirement and Ethics of Online Identity." In *Social Media and the Value of Truth*. Lexington Books.

Facebook. 2013a. "Facebook's Name Policy." https://www.facebook.com/help/292517374180078/.

———. 2013b. "What Types of ID Do You Accept?" *Facebook Help Center*. http://www.facebook.com/help/159096464162185/.

Flatley, Joseph L. 2009. "Sony's PlayStation Eye to Gain Facial Recognition Capabilities." *Engadget*. July 18. http://www.engadget.com/2009/07/18/sonys-playstation-eye-to-gain-facial-recognition-capabilities/.

Google. 2012a. "Google+ Page and Profile Names." October 16. http://support.google.com/plus/answer/1228271?hl=en.

———. 2012b. "Frequently Asked Questions About Google Account and Age Requirements." October 16. https://support.google.com/accounts/bin/answer.py?hl=en&answer=1333913.

———. 2013. "Google Project Glass." *Google Glass*. https://plus.google.com/+projectglass/posts.

Goudelis, Georgios, Anastasios Tefas, and Ioannis Pitas. 2010. "Intelligent Multimedia Analysis for Emerging Biometrics." In *Intelligent Multimedia Analysis for Security Applications*, 97–125.

Gruteser, Marco, and Dirk Grunwald. 2004. "A Methodological Assessment of Location Privacy Risks in Wireless Hotspot Networks." In *Security in Pervasive Computing*, edited by Dieter Hutter, Günter Müller, Werner Stephan, and Markus Ullmann, 2802:10–24. Berlin, Heidelberg: Springer Berlin Heidelberg. http://www.springerlink.com/content/0h4kduy2fxypa3jc/.

ISO - International Organization for Standardization. 2011. "SO/IEC 19794 Information Technology — Biometric Data Interchange Formats". Text. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38749.

Ko, Moo Nam, G.P. Cheek, M. Shehab, and R. Sandhu. 2010. "Social-Networks Connect Services." *Computer* 43 (8) (August): 37–43. doi:10.1109/MC.2010.239.

Lessig, Lawrence. 1998. "The New Chicago School." *The Journal of Legal Studies* 27 (2) (June): 661–691. doi:10.2307/724667.

———. 1999. *Code and Other Laws of Cyberspace*. New York, USA: Basic Books.

Mann, Steve. 2012. "Physical Assault by McDonald's for Wearing Digital Eye Glass." *Steve Mann's Blog*. http://eyetap.blogspot.ca/2012/07/physical-assault-by-mcdonalds-for.html.

Mann, Steve, James Fung, and Raymond Lo. 2006. "Cyborglogging with Camera Phones: Steps Toward Equiveillance." In *Proceedings of the 14th Annual ACM International Conference on Multimedia*, 177–180.

Marx, Gary T. 2013. "Agents Provocateurs." In *The Wiley-Blackwell Encyclopedia of Social and Political Movements*. Blackwell Publishing Ltd. http://onlinelibrary.wiley.com/doi/10.1002/9780470674871.wbespm005/abstract.

Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79: 119.

Ong, Josh. 2013. "China's Baidu Is Testing a Facial Recognition Image Search Engine." *The Next Web*. Accessed March 15. http://thenextweb.com/asia/2012/12/31/chinas-baidu-tests-facial-recognition-image-search-engine/.

Robinson, James. 2012. “Hunting the Craigslist Killer.” *Boston Phoenix*. April 4. http://thephoenix.com/boston/news/136636-hunting-the-craigslist-killer/.

Schneier, Bruce. 2010. “Crowdsourcing Surveillance.” *Schneier on Security*. https://www.schneier.com/blog/archives/2010/11/croudsourcing_s.html.

US Federal Bureau of Investigation. 2009. “Next Generation Identification.” January 26. https://www.fbi.gov/news/stories/2009/january/ngi_012609.

———. 2012. “IAFIS/NGI Biometric Interoperability.” January. https://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngi-interoperability-1.

US Federal Trade Commission. 2012. “FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies: Companies Using the Technologies Should Design Services with Consumer Privacy in Mind.” October 22. http://www.ftc.gov/opa/2012/10/facialrecognition.shtm.

Wang, He, Xuan Bao, Romit Roy Choudhury, and Srihari Nelakuditi. 2013. “InSight: Recognizing Humans Without Face Recognition.” http://www.cse.sc.edu/~srihari/pubs/InSight_HotMobile13.pdf.

Warman, Matt. 2011. “Google Warns Against Facial Recognition Database.” *The Telegraph*, May 18. http://www.telegraph.co.uk/technology/google/8522574/Google-warns-against-facial-recognition-database.html.

Wayman, James L., Anil K. Jain, Davide Maltoni, and Dario Maio. 2005. *Biometric Systems: Technology, Design and Performance Evaluation*. Springer.

Weber, Karsten. 2012. *Surveillance, Sousveillance, Equiveillance: Google Glasses*. SSRN Scholarly Paper ID 2095355. Rochester, NY: Social Science Research Network. http://papers.ssrn.com/abstract=2095355.

Wechsler, Harry. 2007. *Reliable Face Recognition Methods: System Design, Implementation and Evaluation*. Springer.

Wolf, Naomi. 2012. “The New Totalitarianism of Surveillance Technology.” *The Guardian*, August 15. http://www.guardian.co.uk/commentisfree/2012/aug/15/new-totalitarianism-surveillance-technology.

Xuan Zou, J. Kittler, and K. Messer. 2007. “Illumination Invariant Face Recognition: A Survey.” In *First IEEE International Conference on Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007*, 1–8. doi:10.1109/BTAS.2007.4401921.

Yapp, Robin. 2011. “Brazilian Police to Use ‘Robocop-style’ Glasses at World Cup.” *Telegraph.co.uk*, April 12, sec. worldnews. http://www.telegraph.co.uk/news/worldnews/southamerica/brazil/8446088/Brazilian-police-to-use-Robocop-style-glasses-at-World-Cup.html.