



# DIALOGUE

Volume 3 • No. 10 | 2010 September

## FROM THE EDITOR

# Not the Final Word

### IN THIS ISSUE

- 1 *From the Editor*  
Not the Final Word
- 2 *Feature Article*  
Full-Body Scanners:  
Addressing Concerns about  
Wider Deployment
- 4 *Feature Article*  
Biometrics and Privacy in the  
Age of Social Networking
- 6 *News and Notes*

*DIALOGUE* is published quarterly by The Hastings Center, a HIDE Partner.

#### PRINCIPAL INVESTIGATOR

Thomas H. Murray, *President and CEO*

#### EDITOR & PROGRAM MANAGER

Karen J. Maschke, *Research Scholar*

#### ART DIRECTOR

Nora Porter

#### MANAGING EDITOR

Joyce A. Griffin

#### CONSULTING EDITOR

Gregory E. Kaebnick

This work was supported in part by the European Commission under contract FP7-217762 HIDE, Homeland Security, Biometric Identification & Personal Detection Ethics.



Although this is the final issue of *Dialogue*, the newsletter of the HIDE project, it is not the final word about the ethical and privacy concerns regarding biometric technologies. Through focus groups, policy forums, and problem-solving workshops, HIDE partners have established an ongoing dialogue among international and transnational stakeholders on the implications of biometric and personal detection technologies for liberty, security, and democracy. The meeting reports reveal that these stakeholders are committed to improving understanding about the complex ethical and privacy issues these technologies raise. Moreover, they share the goal of identifying common values to serve as the foundation for the use of these technologies in ways that help, rather than harm, individuals, groups, and communities.

As the HIDE project winds down over the next several months, the Web site will continue to be a resource for information about project activities and other developments regarding the ethical and privacy issues of biometric and personal detection technologies. A focus group meeting on technology convergence was held on September 14 in Paris, France. On

October 8, Zuyd University will hold a focus group meeting on embedded technology in Maastricht, the Netherlands. And a final HIDE conference will be held in late 2010 or early 2011. Information about these and other meetings, as well as final project reports, can be found on the HIDE Web site (<http://www.hideproject.org>).

“The HIDE project has established an ongoing dialogue on the implications of biometric technologies for liberty, security, and democracy.”

Finally, to all of the HIDE partners who helped make *Dialogue* an informative source of information about the project and the important issues that were examined over the past two years: Grazi, Danke, Dzienkuje, Merci, Hvala, Bedankt, Thanks!



## FEATURE ARTICLE

# Full-Body Scanners: Addressing Concerns about Wider Deployment

By Ross White, The Hastings Center

On December 25, 2009, a passenger on a flight from Amsterdam to Detroit tried unsuccessfully to ignite an explosive device hidden in his underwear. This recent failed attack of an airplane in flight exposed the limits of traditional airport screening methods to detect nonmetallic substances attached to passengers' bodies or clothes. As a consequence, transportation security officials and others want to expand the use of advanced imaging technologies such as full-body scanners to prevent individuals from boarding commercial aircrafts with dangerous or illegal substances. Although efforts to protect the safety of airline passengers are laudable, the use of full-body scanners raises significant concerns worthy of more discussion. These concerns include the violation of individuals' right to privacy and dignity, the use or misuse of personal information captured by the imaging device, the circumvention of basic human rights, and possible adverse effects on human health (worth mentioning, but not exploring, here).

The European Commission addressed some of these concerns in a report issued in June 2010 in which it advocated for a common European approach for the deployment of full-body scanners in member states. The Commission illuminates some of the concerns raised about the use of security scanners, though it does not go so far as to endorse their increased use.

Nonetheless, the Commission shortsightedly concludes that "security scanner technologies exist that neither produce full-body images nor emit ionizing radiation" and appears willing to disregard many of the most common worries, claiming that "technical standards and operational conditions to be laid down by law could significantly reduce concerns related to fundamental rights and health."<sup>1</sup>

In order to better understand the shortcomings of the Commission's report, it is helpful to explore the issues of protection of privacy, preservation of human dignity, and the use or misuse of personal data. Perhaps the most articulated concern posed by the widespread use of full-body scanners is their ability to reveal a detailed display of the human body, which can expose medical conditions such as prostheses and diapers, various body implants, and other personal anatomical markers and characteristics. Even though the images viewed by airport security personnel are slightly blurred and give more of a general body outline than specific physical details, intimate personal information about the individual being screened that would not otherwise be available from nonimaging technologies will be obtained when using the body scanner.

The Commission acknowledged these concerns but suggested that most of them can be—or already have been—resolved. For example, the

Commission argued that existing technology allows images of the face and/or other body parts not needed for further analysis to be blurred. And it noted that it may be possible to produce a mannequin or stick figure rather than a real image of the body, which does not reveal any actual body parts but only identifies areas of the body to further search.<sup>2</sup>

Current operational measures for full-body screening are designed to separate the person being screened from those reviewing the images. For example, the reviewing officer works remotely from the site where the body is scanned, with no chance of seeing the individual whose image is being viewed and analyzed. This means that it is impossible for the reviewer to link the image to an actual person. Automated communication can further ensure that the information exchanged between the reviewer and the official who is conducting the actual screening is limited to only the information necessary for satisfactory review of the images.<sup>3</sup> In order to minimize discomfort or unease of individuals being screened, some have suggested that the person reviewing the images should be the same gender as the person being screened. Although this heteronormative approach to the screening process is an issue worth mentioning, it will not be explored in depth here.

While these measures to separate the review of images from the actual

screening of the body may help to preserve an individual's anonymity and privacy, the images of that individual could still be stored and viewed later. Scanners may be factory programmed to erase or discard images once they have been used to ensure that passengers do not have potentially dangerous devices on their bodies or in their clothes, but settings on the machine could theoretically be altered to retain images. Even if images are not retained and stored, aggregate data would likely still be stored somewhere in order to gauge the efficacy of the scanners.

Asserting that images will not be stored does not address the fact that individuals are most vulnerable to the risk of their privacy being violated in the moments that they are in the scanner.<sup>4</sup> The potential for individuals to be harmed or to take offense at what others see about their bodies was revealed a few months ago when an employee of the U.S. Transportation Security Agency (TSA) beat a coworker with a baton after the coworker saw a scan of his body and ridiculed him about the size of his genitalia.<sup>5</sup>

Incidents such as this raise serious questions about the detail of the scanned images. Moreover, some individuals have deeper philosophical disagreements with the use of full-body scanners. The most notable are individuals who hold religious beliefs that are incompatible with others viewing their body (whether images are blurred or not). For example, airports in Dubai have already declared that full-body scanners will not be used because they amount to a "virtual strip search," which is inconsistent with national customs and ethics of the largely Muslim population.<sup>6</sup> And some in the United States who oppose use of the scanners have argued that their widespread deployment might violate various legal provisions that protect religious freedom. The use of scanners in the United States might also conflict with the Fourth Amendment of the Constitution, which protects individ-

uals from unwarranted "search and seizure."

Some commentators have asked whether technologies like body scanners sacrifice the right to bodily integrity for the purposes of national security. The HIDE and RISE (Rising Pan European and International Awareness of Biometrics and Security Ethics) projects raised this and other concerns in a recent report on the ethical and policy context of whole-body imaging at airports. The report identifies two different conceptions of bodily integrity: dignitarian and privacy.<sup>7</sup> The dignitarian approach is founded on human beings having a fundamental right to a level of intrinsic dignity. This view derives largely from a human rights perspective articulated in paramount documents such as the Universal Declaration of Human Rights and the Convention on Human Rights and Biomedicine. The privacy conception of human dignity, on the other hand, translates the right to bodily integrity into a more medicosocial model that suggests individuals have a right to bodily autonomy and protection from undue invasion of one's body like that established by the Fourth Amendment to the U.S. Constitution.

While cognizant of these concerns, the U.S. Department of Homeland Security insists that passengers with these concerns can refuse to undergo a full-body scan. But if they do, they must submit to a full-body pat-down by a TSA officer.<sup>8</sup> Some passengers may perceive this process to be even more intrusive than the scanners and may be disinclined to opt for this alternative given the significantly longer time it takes to conduct a physical body check. Moreover, the airports that use full-body scanners might not inform passengers about the opt-out policy because, as the

European Commission suggests, if a significant number of passengers opt for the pat-down instead of the full-body scan, the usefulness of the scanners in terms of their "relation to security, cost and feasibility" might be called into question.<sup>9</sup>

Despite important, unresolved concerns about the further deployment of full-body scanners, their expanded use seems inevitable in the United States. There are currently more than 142 advanced imaging technology units in 41 U.S. airports.<sup>10</sup> In July 2010, the head of the U.S. Department of Homeland Security, Janet Napolitano, announced the deployment of the technology to 28 additional airports using money from the American Recovery and Reinvestment Act of 2009,<sup>11</sup> and the Department of Homeland Security has announced plans to deploy 950

“ There should be a legal framework that describes attributes, capabilities, characteristics, and qualities that allow users to verify whether a system of body scanners is trustworthy. ”

additional units through 2011. Meanwhile, Senators Amy Klobuchar (D-MN) and Bob Bennett (R-UT) recently introduced a bill that would mandate the deployment of full-body scanners in U.S. airports as the primary screening technique.<sup>12</sup>

Given the inevitability of wider deployment of this imaging technology, we must take steps to ensure their safe and controlled integration into airport security practices. As the HIDE/RISE report concludes, the body scanner can be "legitimate as far as it fulfills its original purpose. Any different goal, like people identification or profiling, or detection of anatomic and/or medical details, is not legitimate and is not respectful of

personal integrity.”<sup>13</sup> In order to preserve the right to equality and freedom from discrimination, we must ensure that passengers are not asked to undergo scans based on criteria such as gender, race, color, ethnicity or social origin, or religious or political beliefs.

The HIDE/RISE report also points out that “if we want to implement trusted body scanners, we should define a legal framework and describe attributes, capabilities, characteristics and qualities which allow users to verify whether the systems are trustworthy.”<sup>14</sup> A first step in that direction might include making standard operating procedure manuals available for public view and comment. These operating procedures should clearly state how and what information about the use of scanners will be provided to passengers, including whether passengers can choose not to undergo this type of security screening. If body scanners were to become the primary means of security screening, alternative procedures must remain available, and individuals must also be made fully

aware of their right to choose these alternative screening approaches.

If we decide that using full-body scanners is necessary in the interest of aviation and national security, governments and the organizations that use them must respond more meaningfully to the concerns expressed above. The most useful path forward may be candid and transparent conversations with all who would be affected. This may help assuage fears and make clear the scope of the technology’s use. A failure to do so could lead to a violation of individuals’ right to privacy and human dignity, inappropriate use of their personal data, and more intrusive interventions into their lives if shared security concerns trump personal rights.

1. European Commission. Communication from the Commission to the European Parliament and the Council on the use of security scanners at EU airports. June 2010, p. 18, <http://www.statewatch.org/news/2010/jun/eu-com-body-scanners-com-311-4.pdf>.

2. *Ibid.*, p. 11.

3. *Ibid.*, p. 11-12.

4. HIDE and RISE Projects. Whole body imaging at airport checkpoints: The ethical and policy context. Centre for

Science, Society and Citizenship, February 2010, [http://www.best-nw.eu/\\_fileupload/WG%207/ETHICS%20OF%20BODY%20SCANNER%20POLICY%20REPORT.pdf](http://www.best-nw.eu/_fileupload/WG%207/ETHICS%20OF%20BODY%20SCANNER%20POLICY%20REPORT.pdf).

5. Hunter M. Anatomical ridicule raises body-scanning concerns. CNN, 7 May 2010, <http://www.cnn.com/2010/TRAVEL/05/06/tsa.scanner.assault/index.html>.

6. Shahid A. Full-body scans scrapped at Dubai airports, officials say the device “contradicts Islam.” *New York Daily News*, 6 July 2010, [http://www.nydailynews.com/news/world/2010/07/06/2010-07-06\\_no\\_peeking\\_body\\_scanners\\_scrapped\\_at\\_dubai\\_airports.html](http://www.nydailynews.com/news/world/2010/07/06/2010-07-06_no_peeking_body_scanners_scrapped_at_dubai_airports.html).

7. HIDE and RISE Projects, p. 27-30.

8. Rucker P. TSA tries to assuage privacy concerns about full-body scans. *Washington Post*, 4 January 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/01/03/AR2010010301826.html>.

9. European Commission, p. 18.

10. Transportation Security Administration. Advanced imaging technology, <http://www.tsa.gov/approach/tech/ait/index.shtm>.

11. Department of Homeland Security. Secretary Napolitano announces additional recovery act-funded advanced imaging technology deployments. Press release, 21 July 2010, [http://www.dhs.gov/ynews/releases/pr\\_1279642622060.shtm](http://www.dhs.gov/ynews/releases/pr_1279642622060.shtm).

12. Bennett B, Klobuchar A. Securing aircraft from explosives responsibly. Advanced Imaging Recognition Act of 2010, sec. 3536.

13. HIDE and RISE Projects, p. 5.

14. HIDE and RISE Projects, p. 7.



## FEATURE ARTICLE

# Biometrics and Privacy in the Age of Social Networking

By Polo Black Golde, The Hastings Center

**W**hat does privacy mean when more than 500 million people have posted intimate personal details about themselves in writing or via photos and videos on Facebook? Are privacy concerns about law enforcement and national security officials collecting, storing, and sharing personal and biological information from iris scans, CCTV, DNA samples, or whole-body imaging overblown in the age of online social networking? Is it accurate to assume that people using online social networks are not concerned about privacy in general, and so will not care when biometric technologies are used to collect physical and behavioral information for security purposes?

Privacy concerns are not foreign to Facebook or similar social networking sites. As a result of a recent security breach, the personal details of over 170 million Facebook users ended up on The Pirate Bay, described by the *Los Angeles Times* as “one of the world’s largest facilitators of illegal downloading” of copyrighted content.<sup>1</sup> Once on The Pirate Bay, Facebook information became available to anyone with Internet access. And there have been several backlashes against Facebook in response to various changes in its privacy policies. In April 2009 the company made the information of its 500 million or so users accessible to third-party applications and partner Internet sites. There was so much opposition

from users and privacy advocates that a month later the company revised the service.

The popular press has been quick to split today’s technoconsumers into two camps: the young generation of technophiles for whom privacy concerns are passé, and the older generation of outsiders who are reluctant to release their personal information into cyberspace. Recently this distinction has become less clear-cut. In 2009, the fastest-growing population of Facebook users was at least 55 years old, and the slowest-growing segment was 18- to 24-year-olds. And many commentators have noted that younger Facebook users are increasingly adopting privacy controls over their information posted on the site.<sup>2</sup> In fact, despite the appeal of such a clean dichotomy between generations, the younger generation seems to have quite a varied voice on matters of privacy. Examining this voice shows that it is a matter of where, not whether, the social media generation is expressing privacy concerns.

The generational dichotomy may hold some credence in a sweeping cultural sense. Generation Y was raised amid the evolving paradigm of Internet technology. My elementary

school, in the heart of Silicon Valley, was among the first there to integrate computer lessons into its curriculum. And Apple Inc. donated a computer lab to the school. At the same time, however, my cohort learned to navigate library records using the soon-to-be-obsolete paper card catalog system. Faxes, paper copy, and parcel post had no reliable business alternatives for the majority of my cohort. But my generation was the first as a group to adopt e-mail, instant messaging, and Web browsing, and later, my college cohort was the first to

“ Describing early adopters of Facebook as uniformly unconcerned with privacy overlooks that population’s diversity concerning what and how much they will share. ”

have Facebook available before it expanded to high schools and, ultimately, the general public. At their beginning, these online sources were unreliable, slow, and only ever used for leisure. Because of the coincidence of my generation emerging at the cusp of global information technology, it is the first cohort to fully integrate advanced personal computing into everyday life.

But describing these early adopters

as uniformly unconcerned with privacy overlooks the diversity of that population. For as long as Facebook has been active it has had an increasingly complex array of settings that individual users customize to guide what information they make available to different groups within the online community. Some users are relatively inactive, sharing little by way of personal information and photographs; others are prolific in the amount of information they post. Some of Facebook's early users have always had very careful and restrictive settings to control how many users have access to their information; others have left their information entirely open to the online community. Simply acknowledging the number of individuals with a Facebook account ignores these variations. Additionally, the commercial incentives that push Facebook to encourage its users to display more information publicly—and the inconsistency with which new information-sharing policies have been implemented—has resulted in tension between the company and its customers.

As privacy experts and Internet users alike wrangle with the changing social media landscape, one theory advanced by scholars like Helen Nissenbaum hopes to make room for this quick-paced evolution, recognizing privacy not in terms of abstract rights, but as a matter of contextual integrity. As articulated by Nissenbaum, privacy as contextual integrity is about norms of information flow for particular spaces—like the corporate office or the household backyard—that ought to guide our concerns about the collection, retention, and distribution of personal information. This perspective recognizes the plurality of realms in which we live; in each, different kinds of information are appropriate or fitting to reveal. Nissenbaum mentions that

“distinctive relationships, for example individual to spouse, boss, friend, colleague, priest, teacher, therapist, hairdresser, and so on, are partially defined by distinctive patterns of information sharing. Insofar as these relationships are valued, so would we value adequate and appropriate restrictions on information flows that bolster them.”<sup>3</sup> Nonetheless, she recognizes that some people worry that “contextual integrity, being so tied to practice and convention, loses prescriptive value or moral authority.”<sup>4</sup> With a rapidly changing landscape like that of social media, finding normative footing based on convention is challenging. And though the savvy user may adjust Facebook's privacy settings to his or her satisfaction, the legal implications for the privacy protections regarding the information s/he posts are largely unknown.

The difficulty of identifying what constitutes a violation of privacy in the venue of social media may not lie only in their new and constantly evolving set of practices, but also in the number of contextual spheres in which they interact. On Facebook, each time a user posts a status update, a photo, an announcement of their location, or any new information, she can choose which groups of users can view and interact with that information: she might exclude certain family members from viewing a photo while making it available to all her office colleagues. When examined in this way, prolific (but careful) Facebook users, by detailing their lives on the Internet, may appear not to care about the privacy of their information, but they may in fact be attending diligently to the contexts in which they allow that information to be presented. The governance of informational flow on Facebook may not follow easily delimited categories of professional, familial, social, and romantic, but neither does it ignore

the values and norms of those categories—informational flow can be crafted with more nuance, tuned to particular relationships among individuals.

Concern for privacy may not be absent among social media enthusiasts, but it may have dissolved in a subtler way, in the way that a chemical dissolves in a liquid—maintaining its composition while dispersing finely through its solvent. In the venue of social media, it may be that contextual spheres are parsed out more finely online than they are in other areas of life. How each user handles her sense of risk about a social media platform's external security may be different, especially among the younger generation, for whom there is no uniform voice on this new arena of informational flow. But from private user-to-user messages to network-wide projections of geographic location, even social media enthusiasts seem both to share and to steward their information more diversely than media commentary suggests is the case. Thus, as today's young generation is confronted with biometric technologies that collect biologically-based information—at airport and border security checkpoints, when applying for passport and other identity documents, and when applying for some types of government and private sector jobs—it will be interesting to see how they frame privacy concerns (if at all) in those contexts.

1. Sarno D. The internet sure loves its outlaws. *Los Angeles Times*. 29 April 2007, <http://articles.latimes.com/2007/apr/29/entertainment/ca-webscout29>.

2. Holson LM. Tell-all generation learns to keep things offline. *New York Times*. 8 May 2010, <http://www.nytimes.com/2010/05/09/fashion/09privacy.html>.

3. Nissenbaum H. Privacy as contextual integrity. *Washington Law Review* 2004;79(1):119-158, p. 132.

4. *Ibid.*, p. 126.

**Centre for Science, Society and Citizenship**  
Rome, Italy

**Centre for the Economic and Social  
Aspects of Genomics**  
Lancaster and Cardiff, UK

**Centre for Biomedical Ethics—Yong Loo  
Lin School of Medicine**  
Singapore

**Eutelis Italia SRL**  
Rome, Italy

**Fraunhofer Institute for Computer Graphics  
Research**  
Darmstadt, Germany

**International Biometric Group**  
London, UK

**Optel Ltd**  
Woclaw, Poland

**Sagem Sécurité**  
Paris, France

**The Hastings Center**  
Garrison, NY, USA

**University of Ljubljana**  
Ljubljana, Slovenia

**Zuyd University**  
Heerlen, the Netherlands

## HIDE Upcoming Events

- **8 October 2010**  
Focus Group Meeting on Embedded Technology. Maastricht, the Netherlands.

For an update on HIDE meetings, please visit <http://www.hideproject.org>.

## Recent Publications

- Citron DK and Henry LM. Visionary pragmatism and the value of privacy in the twenty-first century (review of *Understanding Privacy*, by Daniel J. Solove [Harvard University Press, 2008]). *Michigan Law Review* 2010;108:1107-1126.  
<http://www.michiganlawreview.org/assets/pdfs/108/6/citronhenry.pdf>
- European Commission. Communication from the Commission to the European Parliament and the Council on the use of security scanners at EU airports. June 2010.  
<http://www.statewatch.org/news/2010/jun/eu-com-body-scanners-com-311-4.pdf>
- Hoffman S. Biometrics, retinal scanning, and the right to privacy in the twenty-first century. *Syracuse Science & Technology Law Reporter* 2010;22:38-52.  
[http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=stephen\\_hoffman](http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=stephen_hoffman)
- Liu Y. Privacy regulations on biometrics in Australia. *Computer Law & Security Review* 2010;26(4):355-367.
- London Economics. Study on the economic benefits of privacy enhancing technologies (PETs): Final report to The European Commission DG Justice, Freedom and Security. July 2010.  
[http://ec.europa.eu/justice/policies/privacy/docs/studies/final\\_report\\_pets\\_16\\_07\\_10\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf)
- Lwin M. Privacy issues with DNA databases and retention of individuals' DNA information by law enforcement agencies: The holding of the European Court of Human Rights case *S and Marper v. United Kingdom* should be adapted to American Fourth Amendment jurisprudence. *Information & Communications Technology Law*. 2010;19(2):198-222.
- Schartum DW. Designing and formulating data protection laws. *International Journal of Law and Information Technology* 2010;18(1):1-27.  
<http://ijlit.oxfordjournals.org/cgi/content/full/ean013>