Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy

March 2009

Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy

Whole Body Imaging (WBI) technologies are being deployed as a passenger scanning measure in a growing number of airports in order to complement, and at times replace, other security technologies such as metal or explosive detectors.[1,2] Described in the press as a "naked scanner," these technologies have the ability to produce high-quality images of the naked body beneath a passenger's clothes.[3] Improved airport security, however, need not come at the expense of privacy – both may be achieved together in a positive-sum (not zero-sum) manner. This paper will describe the possible means for WBI to rise above its negative privacy connotations and become what we are calling, a *Transformative Technology*. We believe that the privacy-invasive potential of Whole Body Imaging must be squarely addressed in the design phase of the technology, as well as in its deployment and use, with attention to physical privacy and adequate privacy processes.

Transformative Technologies

In 1995, the Ontario Information and Privacy Commissioner (IPC) and the Dutch Data Protection Authority coined the acronym *PETs*, for Privacy-Enhancing Technologies. This term refers to coherent systems of information and communication technologies that strengthen the protection of privacy in information systems by preventing the unnecessary or unlawful collection, use, and disclosure of personal data, or by offering tools to enhance an individual's control over his or her data. PETs are the technological embodiment of the universal privacy principles contained in fair information practices.

In 2008, my office extended the idea of PETs to PETs *Plus*[4], creating the new concept of *Transformative Technologies*[5]. Dissatisfied with the "zero-sum" paradigm of security *vs.* privacy, in which gains in security are met with corresponding losses in privacy (and vice versa), we embraced the notion of a *positive-sum* paradigm,

[1] Paul Giblin and Eric Lipton, "*New Airport X-Rays Scan Bodies, Not Just Bags,*" The New York Times, Feb 24, 2007: **www.nytimes.com/2007/02/24/us/24scan.html**

[2] **http://en.wikipedia.org/wiki/Puffer_Machine**

[3] Carly Weeks, "*Critics blast new airport superscan,*" Globe and Mail, June 25, 2008. p. L1.

[4] Cavoukian, Ann, Ph.D., Moving Forward from PETs to PETs Plus: *The Time for Change is Now* at: **www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=834**

[5] Cavoukian, Ann, Ph.D., *Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum*, at: **www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=758**

in which *all* parties can benefit from technological advances. In this paradigm, privacy protections are incorporated into security technologies from the outset, hence the Commissioner's term, "Privacy by Design."[6] Applying a PET to a surveillance technology, while maintaining the goal of a positive-sum paradigm, can create a "Transformative Technology" because it can, in effect, transform an otherwise privacy-invasive technology into a privacy-protective one.

Positive-Sum Paradigm + Privacy-Enhancing Technology = Transformative Technology

Virtually any privacy-invasive surveillance or security technology can be turned into a *Transformative Technology*, and Whole Body Imaging is no exception.

Whole Body Imaging

Whole Body Imaging technology involves a process by which various imaging techniques are used to scan and create a full-body (two- or three-dimensional) image of an individual, including the surface of the skin and objects on, but not in, the body. Currently, the scan is conducted using one of two technologies:

Backscatter, which uses the reflections from a low-intensity X-ray beam to construct a two-dimensional (2-D) image, or

Millimetre-wave, which uses non-ionizing radio frequency energy in the millimetre-wave spectrum to detect energy reflected from the body to construct a three-dimensional (3-D) body image.

The stated goals of the use of WBI technologies for passenger screening are twofold: first, such imaging is reported to be superior in its ability to detect both metallic and non-metallic threat objects; second, airport authorities believe that this procedure will be the preferred choice to physical pat-downs or strip searches for individuals undergoing security screening.

A number of trials have already been undertaken to evaluate the effectiveness of WBI technology for secondary passenger screening at airports.[7] In the United States, WBI was tested at Phoenix, Boston, Chicago, Las Vegas, Kansas City, Los Angeles, Miami, Tampa, and at JFK Airport in New York, among others. The U.S. Transportation

[6] "Privacy by Design" is a term coined in the '90s by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, in an effort to enlist the support of technology to protect privacy, rather than encroach upon it. For more details, see her *Privacy by Design* paper, at: **www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=835** or go to: **www.privacybydesign.ca**

[7] Although both types of scanning technologies are effective at detecting aviation threat objects, it is predominantly millimetre-wave rather than backscatter systems that are being deployed at airports. The main reasons for this predominance appear to be twofold: (a) preference for using radio waves instead of X-rays and (b) faster passenger processing by the millimeter-wave machines. Both systems, however, can produce highly detailed and identifiable images of the naked body, absent the use of strong privacy filters.

Security Administration (TSA) intends to deploy 120 machines in 23 locations nationwide by the end of 2009.[8] Similar trials were undertaken in India (New Delhi), Australia (Sydney, Melbourne and Adelaide), Japan (Osaka), Russia (Moscow), the Netherlands (Amsterdam's Schiphol) and at London's Heathrow Airport in 2004.[9,10]

After testing WBI in 2006, the organization responsible for security at India's airports – the Central Industrial Security Force (CISF) rejected the use of the machines. The CISF claimed that the images the machines produced were too revealing and would offend passengers, as well as embarrass their security officials.[11]

Scrutiny is increasing. In September 2008, the European Commission, part of the European Union's (EU) executive branch, proposed adding the machines to a list of security measures used in EU airports, saying that the scanners would not be used routinely on passengers, and would provide a less intrusive alternate to strip-searching. The proposal was withdrawn after the European Parliament ruled that the scanners "have a serious impact on the fundamental rights of citizens" and voted overwhelmingly for additional study on the privacy and safety implications. The Commission said it will continue examining how the scanners can be used in consultation with the European Data protection Supervisor (EDPS), the Article 29 Working Party and the Fundamental Rights Agency, and "is now in the process of drawing up a package of rules for how the scanners will be deployed.[12]

Meanwhile, the U.S. TSA has proceeded to Phase 2 of its deployment strategy, that is, using WBI for *primary* screening, On January 19, 2009, *USA Today* reported that, "For the first time, some airline passengers will skip metal detectors and instead be screened by body scanning machines that look through clothing for hidden weapons."[13] This will be taking place at Tulsa International Airport, followed by airports in San Francisco, Las Vegas, Miami, Albuquerque, and Salt Lake City. "Passengers at the test airports will be instructed to go through the new scanners. Anyone who doesn't want to go through will be allowed to refuse and instead go through a metal detector and receive a pat-down."

[8] **www.tsa.gov/approach/tech/body_imaging.shtm**

[9] **www.timesonline.co.uk/tol/news/uk/article504009.ece**

[10] **www.glgroup.com/News/Using-backscatter-X-ray-on-passengers-at-airports-8202.html**

[11] **www.cnn.com/2007/TRAVEL/03/06/bt.backscatterxray/index.html**

[12] European Parliament resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection: **http://tinyurl.com/bar8ag**

EU gives up airport "strip search" scans, Reuters, Nov 19, 2008, at: **http://uk.reuters.com/article/topNews/idUKTRE4AI6KN20081119**

Germany rejects full-body scans at airports, CBC News, October 24, 2008 at: **www.cbc.ca/world/story/2008/10/24/germany-xray.html**

[13] Frank, Thomas, "*Body scanners replace metal detectors in tryout at Tulsa airport,*" USA Today, February 18, 2009, at: **www.usatoday.com/travel/flights/2009-02-17-detectors_N.htm**

In July 2008, the Canadian Air Transport Security Authority (CATSA) began a seven-month trial of millimetre-wave scanning technology for voluntary primary screening of passengers at Kelowna International Airport.[14]

Technology: Obfuscation

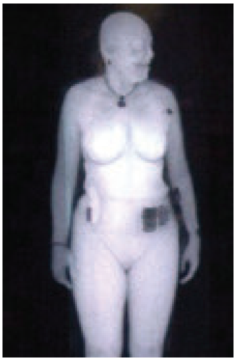

Figure 1

By themselves, both backscatter and millimetre-wave technologies produce highly detailed images, as illustrated by Figures 1 (at left), 2 and 3 (below).

This has led to the popular conception of WBI as a "virtual strip search." Developers and users of these technologies have recognized this as an issue that must be addressed. A number of algorithms or privacy ("modesty") filters have been developed with the goal of reducing or eliminating the level of personal detail contained in the images displayed to screeners, while simultaneously highlighting objects carried on the person. Thus, a wide range of potential images may be presented to screeners, ranging from detailed and identifiable to generic and unidentifiable.

Figure 1, above, is a widely distributed image of the director of the TSA's security laboratory, who had consented to having her body X-rayed by the "backscatter" scanner at the U.S. Transportation Security Administration in 2003.[15] This image demonstrates a raw, unfiltered backscatter image with no privacy filter applied.

Figures 2 and 3, to the right, are images created by millimetre-wave technology, which produce holographic black and white silhouettes. In the first frame a woman stands in standard screening pose, that is, legs apart with hands held over the head; in the second, a man is holding a half-filled bottle of water[16]. Privacy can be protected by using system options that display obfuscated images (e.g., by blurring facial features [Figure 2] and private areas [Figure 3].)

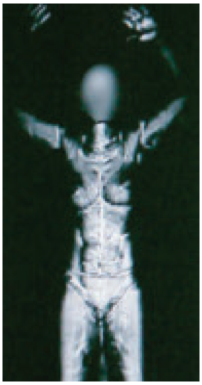

Figure 2

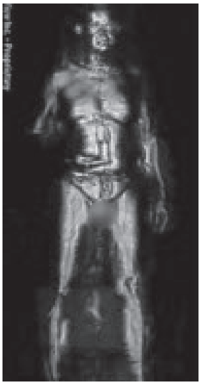

Figure 3

[14] www.catsa-acsta.gc.ca/english/media/rel_comm/2008-06-19.shtml

[15] Credit: AP Photo/Brian Branch-Price, *Nice Bombs Ya Got There,* Wired, June 26, 2003 at: **www.wired.com/science/discoveries/news/2003/06/59401#**

[16] Photos by L-3 Communications as provided to Corrections.com and accessed at: **http://picasaweb.google.com/correctionsconnection/MillimeterWaveTechnology #5178699965699051458**

Although both types of scanning technologies are effective at detecting aviation threat objects, it is predominantly millimetre-wave rather than backscatter systems that are being deployed at airports. The main reasons for this predominance appear to be twofold: (a) preference for using radio waves instead of X-rays; and (b) faster passenger processing by the millimetre-wave machines. Both systems can, however, produce highly detailed and identifiable images of the naked body, absent the use of strong privacy filters.

Millimetre-Wave Privacy Algorithms

In 2002, the IPC became aware of research undertaken by the U.S.-based Pacific Northwest National Laboratory (PNNL) with regards to privacy and 3-D body scans[17]. In conjunction with their work on the millimetre-wave scanner (the "Personal Security Scanner"), the PNNL's research team recognized that a natural objection to the adoption of this technology was the potential for the display of body details. They thus developed a privacy algorithm whose goal was to "… eliminate from the imagery, all human features that may be considered too intrusive."[18]

The privacy algorithm initially developed was based on a technology called "speckle detection."[19] The researchers found that plastics, ceramics, and other dielectric (i.e., non-conducting) materials are partially transparent to millimetre-wave insulation. This leads to a speckled texture in the scanned image, which appears visually as a granulated segment where the threat is located. Human skin, on the other hand, appears with a very smooth texture in millimetre-wave scans, with little pixel-to-pixel variation. Taking advantage of this difference, the researchers developed a neural network-based algorithm that examined various segments of the image for this granular texture, performing a series of post-processing tasks on "speckled" segments to reduce noise and false positives. It was determined that that this algorithm was as effective at identifying threat objects as were trained human examiners who viewed the same images. Once threat objects were determined, the PNNL's algorithm was able to indicate their locations in a number of ways, including on a 3-D rendering of a generic human form, which is especially important to this discussion.

[17] Cavoukian, Ann, Ph.D., *Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift* (2002) at:
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=245

[18] Keller, P. et al. "Privacy Algorithm for Airport Passenger Screening Portal." *Applications and Science of Computational Intelligence III*. (1999) Vol. 4055, pp. 476-483. at:
www.cc.gatech.edu/grads/s/Jay.Summet/papers/keller_SPIE_v4055_i3_2000_p476_.pdf

[19] *Ibid*, pp. 476-483.

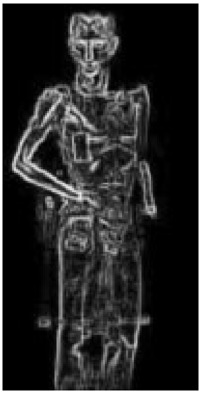

Figure 4

Figure 4 (at left) illustrates the application of privacy-enhancing morphological edge and gradient detection software algorithms, developed by PNNL researchers, applied to WBI holographic millimetre-wave images.[20] This technique goes far beyond simply masking the face and the genitals – it obscures the personal details associated with the entire body. PNNL researchers also developed other approaches to obscuring passenger image details.[21]

In 2008, the IPC contacted the PNNL researchers, inquiring about any updates to their work. We were informed that PNNL privacy research in this area had been acquired in 2002 by Safeview, developers of "advanced technologies for the protection of people and property," and later in 2006 by L-3 Communications, marketers of ProVision Checkpoint millimetre-wave passenger scanning technologies. However, it remains unclear what use, if any, L-3 Communications have made of PNNL's privacy algorithms. The L-3 ProVision Whole Body Imager FAQ states only that "[p]rivacy can be … protected by using system options that allow for further blurring of facial features and blurring of private areas."[22] In conversations with L-3, they indicated they had no plans to incorporate this innovative privacy algorithm into their scanners.

Similar privacy-enhancing options are offered by Rapiscan Systems WaveScan 200 millimetre-wave scanners, sensors for which, according to the company, "do not image anatomical details, thus protecting privacy."[23]

Other laboratories have also been working on the development of privacy algorithms. Researchers, working at Carnegie Mellon's CYLAB[24], have developed a means of blurring or making transparent "sensitive" areas of the human body, rather than removing all the details. This is accomplished by creating a detailed understanding of intrinsic human proportions, and using this data to limit the algorithmic search area for head, chest, and genital regions; once these areas are identified, various blurring and/or transparency filters can be applied.

[20] Paul E. Keller, Douglas L. McMakin, David M. Sheen, A. David McKinnon, Jay W. Summet, *Privacy Algorithm for Cylindrical Holographic Weapons Surveillance System,* (2000) Pacific Northwest National Laboratory, available at: **www.pnl.gov/nsd/commercial/scanner/papers/carnahan.pdf**

[21] *Ibid,* (See also #18 and U.S. Patent 7365672 – *Detection of a concealed object* at: **www.patentstorm.us/patents/7365672/description.html)**

[22] **www.dsxray.com/pdf/ProVisionFAQSEPT08.pdf**

[23] **www.rapiscansystems.com/rapiscan-wavescan-200.html** and also **www.rapiscansystems.com/datasheets/Rapiscan-WaveScan-200-Brochure.pdf**

[24] Laws, J. et al. "Feature hiding in 3-D human body scans." *Information Visualization*. (2006) Vol. 5, pp. 271-278.

Backscatter Privacy Algorithm

Privacy algorithms for backscatter images, which are two-dimensional (as opposed to the 3-D images of millimetre-wave scanning), endeavour to reduce human features to the level of a "chalk outline."[25] The system "creates an image that looks like a chalk outline of the passenger with threats outlined, but does not reveal facial features" (see Figure 5 below), according to American Science and Engineering (AS&E), manufacturer of the SmartCheck Z Backscatter Personnel Screening System used by the Transportation Security Administration. Additionally, company information notes that "the SmartCheck systems installed at JFK, LAX and Phoenix Sky Harbor cannot store, export, print or transmit images."[26]

Figure 5, below, shows a sample backscatter image from an AS&E machine, run through their privacy filter.[27] Outline images such as these are far more privacy-protective and thus preferable to the image shown in Figures 1, 2 and 3.

Activate the Privacy Filter

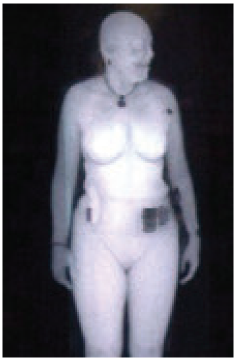

Figure 1

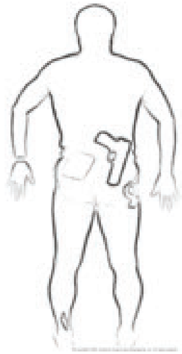

Figure 5

Governments, public officials, and vendors of WBI must ensure that privacy filters obscuring bodily details are available and activated, and that all personnel operating these scanners are trained in their use. When faced with the choice of having the image in Figure 1 vs. Figure 5 appear, I believe that most people would opt for Figure 5, which obscures all personal bodily details. Why wouldn't governments select Figure 5, which only displays an outline of the physical form but yet clearly reveals any and all concealed objects? The choice is clear, and yet there has been very little discussion of the "privacy filters" available for use with Whole Body Image scanners. They represent a positive-sum, privacy-enhancing technology, that can be truly transformative in nature. But first, they must be used – we must ask that strong privacy filters, as illustrated in Figures 4 and 5, be installed and activated.

[25] **www.as-e.com/products_solutions/tsa_z_backscatter_pilot.asp**

[26] **www.msnbc.msn.com/id/26408850/**

[27] Figure source from AS&E Inc. at: **www.as-e.com/products_solutions/tsa_z_backscatter_pilot.asp**

WBI and "Privacy by Design"

In addition to ensuring that strong privacy algorithms are applied to WBI technology, other design and operational factors, such as physical design and program practices, are also critical to a Privacy by Design approach.[28]

In particular, there must be a complete prohibition against any retention or transmission of the images in any format.[29] This policy and practice may also require audits and other assurance methods in order to ensure compliance, thereby engendering public confidence and trust. Bruce Schneier, a security technology expert and noted author, said that the machines strike an "excellent" balance between privacy and security, but adds "the issue we're worried about is whether they save the images."[30]

Another important factor is who actually sees the WBI images, and when. Airport authorities in Canada and the U.S. have created separate image viewing rooms (in remote back rooms), where security personnel cannot see the scanned passengers before or after the scans, and do not have access to passenger details. These personnel are also banned from bringing photographic devices (including cellphones) into the viewing area and are prohibited from connecting storage or communication devices to the machine. We applaud this approach.

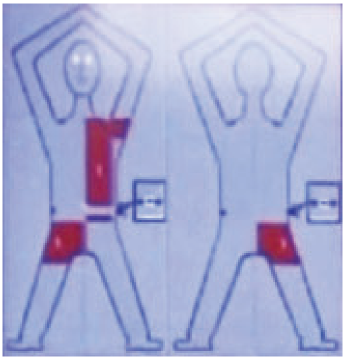

Figure 6

When security screeners in the remote "backroom" notice an anomaly or detect a potential threat in the WBI images, they can communicate this information in real time to "front line" screening personnel (who are actually out front, next to the passengers) through a different graphical interface, such as the one shown at left in Figure 6, developed by CATSA for use in Kelowna. The TSA has developed a similar interface for front-line screeners. Here, you can see that areas of the body requiring further inspection by front-line screeners are highlighted on a generic body outline, with no physical bodily parts actually seen. Additional information, if needed, can be shared between screeners via discreet radio communications. This is an excellent privacy practice that supports image obfuscation, and should go a long way towards alleviating the privacy concerns of passengers actually interacting with airport screening officials.

[28] U.S. Department of Homeland Security, *Privacy Impact Assessment for TSA Whole Body Imaging,* October 17, 2008 at: **www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbi.pdf**

[29] **www.msnbc.msn.com/id/26408850/**

[30] **www.usatoday.com/news/washington/2007-10-07-backscatter_N.htm**

We also note that participation in the system is voluntary and mainly used for secondary screening purposes at this time. However, as noted earlier, WBI is starting to be used for primary screening as well. Travellers who are uncertain or uncomfortable should have the complete freedom to choose not to submit to the image screening, without being required to provide a reason or being subjected to any penalty, and to opt instead for traditional metal detectors.

Ultimately, it comes down to public confidence and trust that the minimum information required will be captured by system operators and used responsibly to make decisions affecting travellers. Clear and transparent rules affecting system design and operation, supported by credible assurance methods, will go a long way in this regard.

Conclusion

Whole Body Imaging technologies that incorporate strong privacy filters – rendering bodily images to mere outlines, to front-line screeners (Figures 5 and 6), can deliver privacy-protective security. When combined with appropriate viewing, usage and retention policies, privacy algorithms that obscure personal details, while still allowing potentially threatening concealed objects to be revealed, will allow WBI implementations to satisfy security requirements without sacrificing (and perhaps enhancing) passenger privacy. We believe that this positive-sum paradigm can, and should be, the end goal of such airport security passenger screening technologies – security *and* privacy, not one at the expense of the other.