

Privacy Issues of Imaging Technologies for Security Search Applications

Claudia Diaz

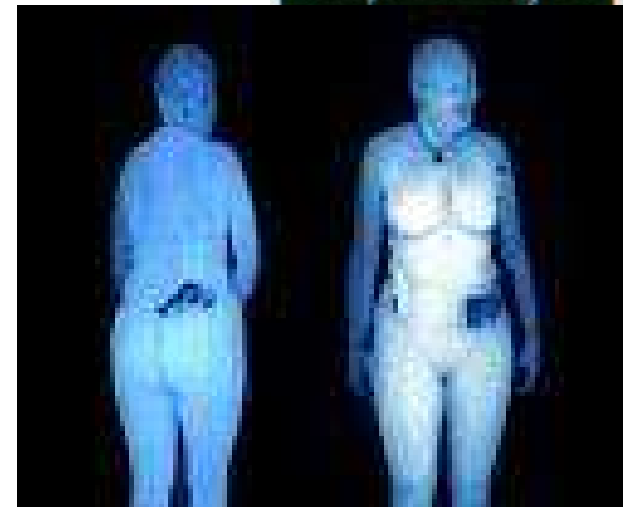
K.U.Leuven LICT (COSIC)

Overview

- Whole body imaging and airport security
- The privacy debate
 - US Transportation Security Administration (TSA)
 - EU policy makers
 - Privacy activists
- Translation of classical privacy threats from academic technical research
- Privacy-preserving body imaging?
- Conclusions and open questions

Whole body imaging

- Detects both metallic and nonmetallic threat items
- Two technologies:
 - Backscatter X-Ray
 - Millimeter wave
- Deployment:
 - *“There are now [in the USA] 40 machines being used in 19 airports”* [TSA, May 2009]
 - Airports in the United Kingdom, Spain, Japan, Australia, Mexico, Thailand and the Netherlands



Airport security

- Advantages [TSA, May 2009]:
 - **Effective:** *“It is proven technology, and we are highly confident in its detection capability”*
 - **Fast:** *“A body scan takes **between 15 and 30 seconds**, while a **full pat-down** can take from two to four minutes” (plus being touched)*
 - **Convenient:** *“When given the choice, ‘over **99 percent** of passengers choose this technology over other screening options’”*
 - **Safe:** *“...millimeter wave technology, which the TSA says emits 10,000 times **less radio frequency than a cell phone**”*

Addressing privacy concerns...

- The system uses a **pair of security officers**. The one working the machine never sees the image, which appears on a computer screen behind closed doors elsewhere; and the remotely located officer who sees the image never sees the passenger
- A passenger's face is blurred and the image as a whole “**resembles a fuzzy negative**”
- The officers monitoring images are **not allowed** to bring cameras, cell phones or any **recording device** into the room
- The computers have been programmed so they have “**zero storage capability**”
- Images are “**automatically deleted**”

What about Europe?

- September 2008: European Commission proposes to add the machines to a list of security measures used in EU airports
 - Proposal was meant to harmonize the conditions in which they can be operated
- October 2008: European Parliament votes against authorizing their use in European airports. The vote was 361 to 16 against the scanners.
 - “the measures foreseen cannot be considered mere technical measures related to security, but have a **serious impact on the fundamental rights of citizens.**”
 - The European Parliament resolution does not call for an **outright ban** on such scanners
 - Postponing the decision: “additional study on the privacy and safety implications of the scanner”
 - Article 29 WP drafting rules “for *how* the scanners *will* be deployed”

Stronger reactions

- Germany, Interior Ministry
 - *“No matter what the EU decides, they will never appear in German airports”*
 - *“We will not take part in this nonsense”*
- India
 - Machines rejected after testing because the images were “too revealing, would offend passengers, and embarrass security officials”

Concerns of EU policy makers

- Health impact
 - Medical and health implications of repeated exposure (e.g., airport personnel)
 - Medical conditions such as pregnancy, chronic diseases
 - Children (under-12s not scanned)
- Data protection
 - Proportionality principle: data must be relevant, adequate, and non-excessive
 - Rights of access?
- Human rights, privacy, personal dignity

Human rights, personal dignity

- Nudity an issue for most people, also MEPs:
 - *“It is unacceptable, if scanners are used; these are machines that see you completely naked”*
 - *“These devices allow one to see genitals, if a woman has big or small breasts”*
- Undignifying, sense of vulnerability
 - *“I think this is an offense against human dignity”*
 - *“This technology has the potential – and, I stress, the potential – to force air passengers to undergo what could be seen as undignifying treatment, and this is certainly not a small technical step”*
 - Does the individual undergoing the check perceive it as something that increases his/her safety, or rather the opposite?
 - *“Forced nudity”* has awful associations (to HR abuses)

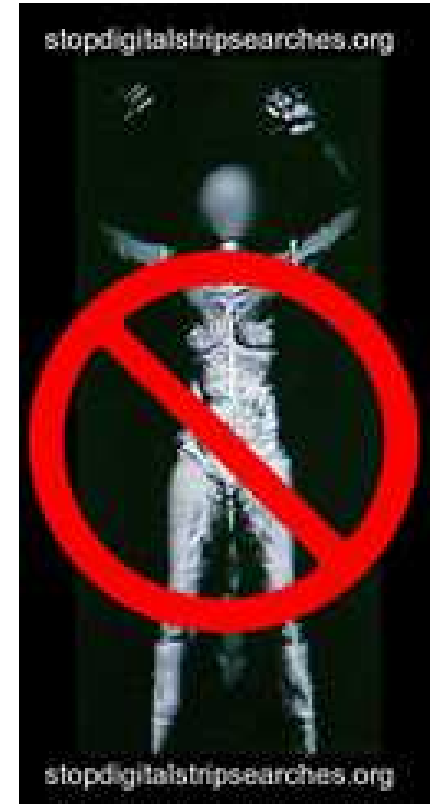
Better than a pat-down?

- Lawyer with the American Civil Liberties Union:
 - *“A choice between being groped and being stripped, I don't think we should pretend those are the only choices. People shouldn't be humiliated by their government in the name of security, nor should they trust that the images will always be kept private”*

What privacy activists are saying: image quality

- Image quality [**“resembles a fuzzy negative”**]:
 - *“What they're showing you now is a dumbed-down version of what this technology is capable of doing”*
 - *“What's to stop TSA from using clearer images or different technology later?”*

Stop Whole Body Imaging



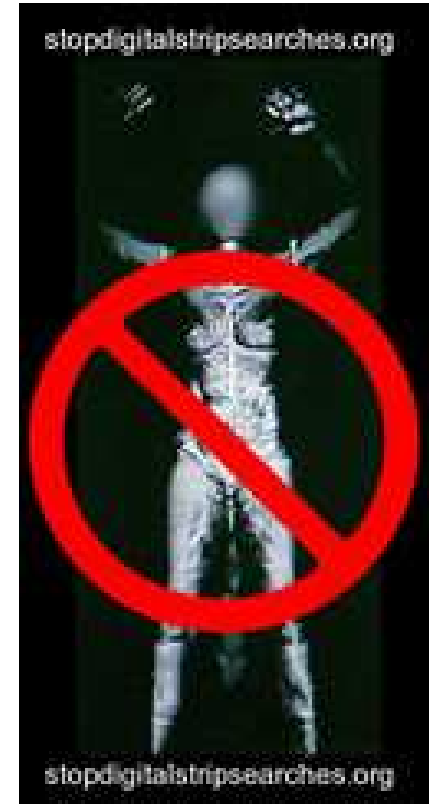
The Privacy Coalition –
EPIC (Electronic Privacy
Information Center)

July 9, 2009

What privacy activists are saying: image recording

- Image recording [**“zero storage capability”**]:
 - *“The TSA said that the image-recording feature would be **disabled**, it is obvious that the devices are designed to capture, record, and store detailed images of individuals undressed”*
 - *“If a passenger were found with anything suspicious under their clothes, you can bet the TSA would need to supply proof”*
- Image recording [**“no cameras allowed”**]:
 - *“Many of us have mobile phones or have these little cameras. There is nothing in this technology that would prohibit the recording of these. With 45,000 good, hardworking TSA employees, 450 airports, some two million air traffic travelers a day, **there is inevitably going to be a breach of security.**”*

Stop Whole Body Imaging



The Privacy Coalition –
EPIC (Electronic Privacy
Information Center)

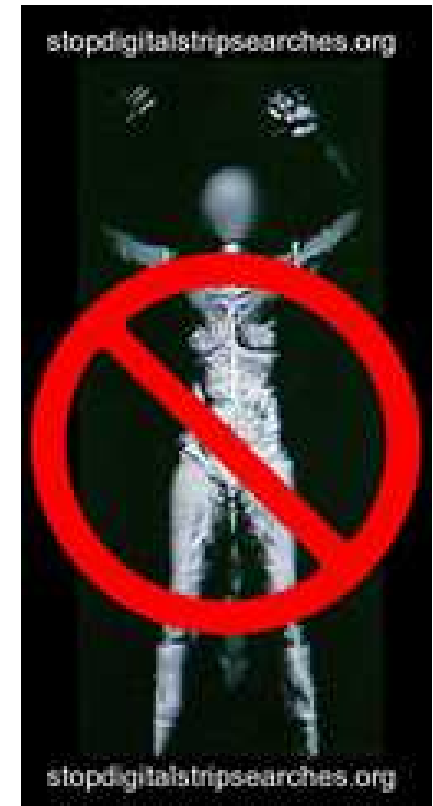
July 9, 2009

What privacy activists are saying: image dissemination

- **Image dissemination**

- *“The images produced could one day be circulated on the Internet”*
- *“Screeners at LAX [Los Angeles International Airport] could make a fortune off naked virtual images of celebrities.”*

Stop Whole Body Imaging



The Privacy Coalition –
EPIC (Electronic Privacy
Information Center)

July 9, 2009

Effectiveness?

- Bruce Schneier believes money would be better spent on intelligence-gathering and investigations
 - *“It's stupid to spend money so terrorists can change plans. If terrorists are swayed from going through airports, they'll just target other locations”*
- Rep. Chaffetz, R-Utah, has proposed a bill to stop whole-body imaging scanners being used as the primary source of TSA security (May 2009)
 - *“Nobody needs to see my wife and kids naked to secure an airplane”*
- MEPs
 - *“Using this technology does not make us safer”*
 - *“The idea is proof of the ‘paranoia of interior ministers’ when it comes to the question of fighting terrorism”*

Slippery slope

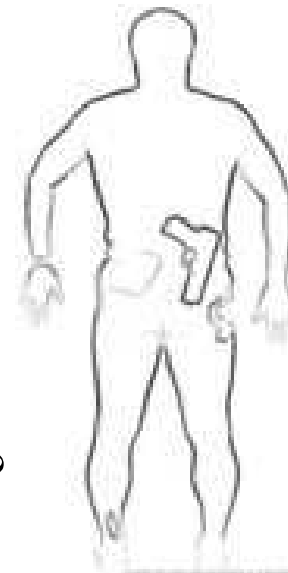
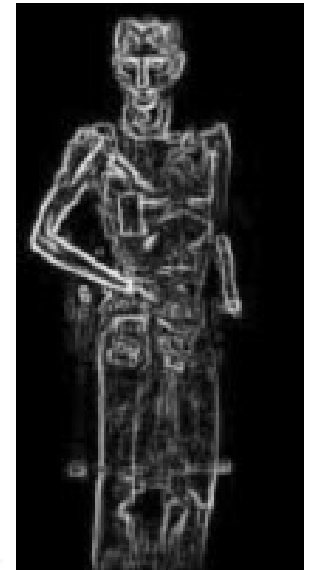
- Concerns over the TSA changing policy down the road
 - Better quality images, start recording them, find some new use for them
 - Privacy advocates want more **oversight, full disclosure** for air travelers, and **legal** language to protect passengers and prevent policy changes
- Concerns over the spread of the technology
 - *“As the equipment gets cheaper, it will become more pervasive and harder to regulate. I wonder whether the machines will someday show up in malls.”*
- Concerns over secondary use (next slide)

Extrapolating threats from academic privacy research

- Profiling and discrimination, using images to infer information about:
 - Ethnic group
 - Medical conditions (thermal cameras already used to detect people infected with flu)
 - Religion (e.g., circumcision)
 - Sexual orientation
 - Politics (e.g., people trying to leave Tehran these days with certain types of injuries are likely to be protesters)
- Re-identification of individuals (biometrics)
 - Checking against a (biometric) database of suspects?
 - Medical info interesting to sell to health insurance companies – “preexisting conditions”
- Technical measures to prevent modifications
 - e.g., tamper resistance
- Trust assumptions and incentives of each of the stakeholders
 - e.g., possible to bribe a security officer to get some pictures?

Privacy-preserving body imaging?

- Privacy “filters”: Processing of raw images to filter out details (face, genitals), human sees result
- More recent designs work on an alarm system - a red light flashes or an alarm sounds if an unexpected object is detected beneath clothing (no human looking at the images at all)
- Is the question of whether or not a **human** is viewing the images *the* crucial one? Are we ‘ok’ privacy-wise if only a **machine** can see us naked?



Conclusions

- This is a controversial topic
- Not clear who will win the debate. May depend on which of these two things happens first:
 - A security breach involving pictures of naked people appearing in the Internet
 - A major airport-related terrorist attack
- Open questions:
 - Can we reconcile air travel security and respect for people's privacy?
 - Which is the right combination of legal and technical measures to prevent abuse?
 - Are we *really* improving (national) security? How much? Is the improvement worth the price in individual freedom / dignity?
 - Would this question be relevant in the aftermath of a terrorist attack?
 - Is this the beginning of a slippery slope?