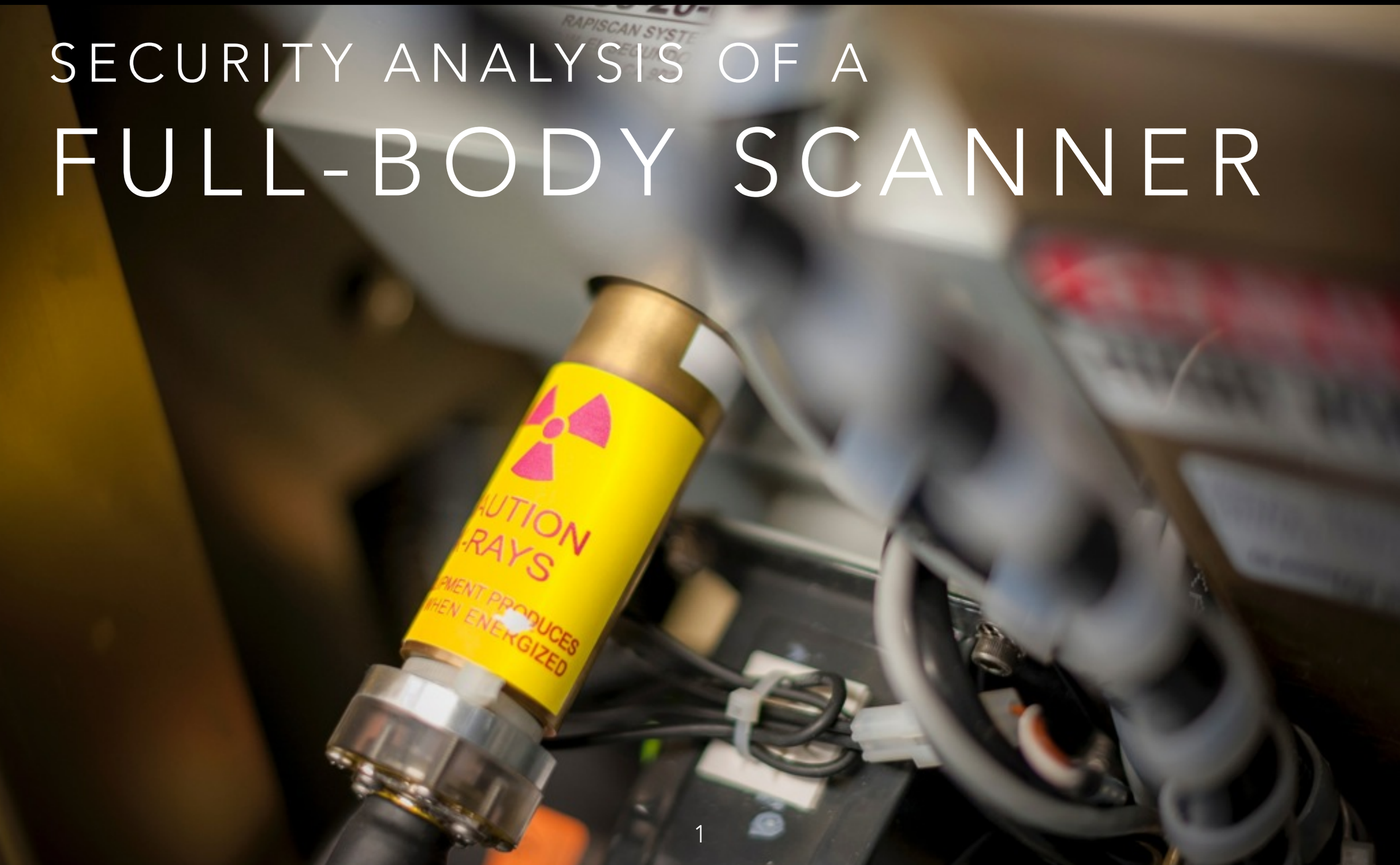
KEATON MOWERY, ERIC WUSTROW, TOM WYPYCH, COREY SINGLETON,
CHRIS COMFORT, ERIC RESCORLA, STEPHEN CHECKOWAY,
J. ALEX HALDERMAN, HOVAV SHACHAM
UNIVERSITY OF CALIFORNIA, SAN DIEGO • UNIVERSITY OF MICHIGAN • JOHNS HOPKINS UNIVERSITY

# SECURITY ANALYSIS OF A FULL-BODY SCANNER



**Warning: Nudity**

talk shows unmodified scanner images to demonstrate the privacy implications of full body scanning

# FULL BODY SCANNERS



Rapiscan® systems




IMAGE: RAPISCAN CORP., L-3 COMMUNICATIONS

# FULL BODY SCANNER DEPLOYMENT

2007 2008 2009 2010 2011 2012 2013 2014



Rapiscan® systems

L3

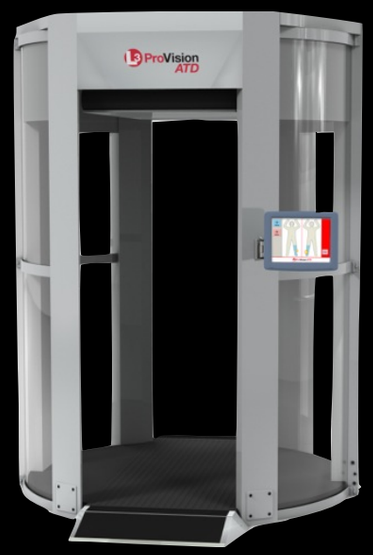



IMAGE: RAPISCAN CORP., L-3 COMMUNICATIONS

# FULL BODY SCANNER DEPLOYMENT

2007 2008 2009 2010 2011 2012 2013 2014

Feb 2007:
TSA introduces FBSs as
‘secondary screening’



Rapiscan® systems

L3

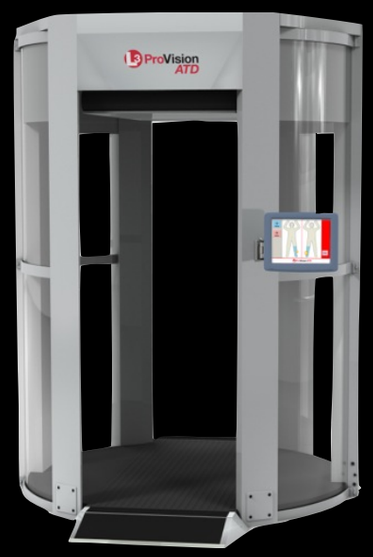



IMAGE: RAPISCAN CORP., L-3 COMMUNICATIONS

# FULL BODY SCANNER DEPLOYMENT

2007 2008 2009 2010 2011 2012 2013 2014

Feb 2007:
TSA introduces FBSs as ‘secondary screening’

Dec 2009:
Failed bombing of Transatlantic flight



Rapiscan® systems

L3

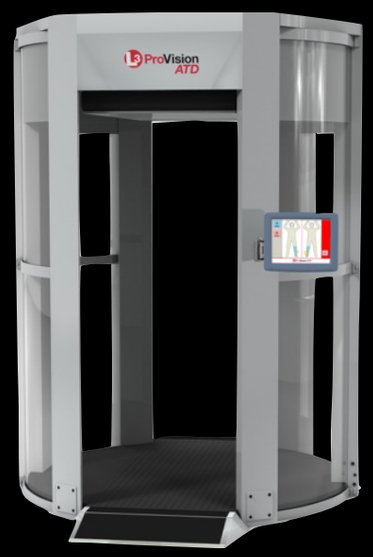



IMAGE: RAPISCAN CORP., L-3 COMMUNICATIONS

# FULL BODY SCANNER DEPLOYMENT

Dec 2009:
TSA moves FBSs to
primary screening

2007 2008 2009 2010 2011 2012 2013 2014

Feb 2007:
TSA introduces FBSs as
‘secondary screening’

Dec 2009:
Failed bombing of
Transatlantic flight



Rapiscan® systems

L3

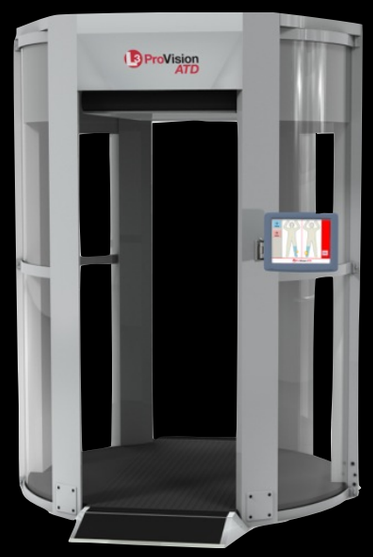



IMAGE: RAPISCAN CORP., L-3 COMMUNICATIONS

# FULL BODY SCANNER DEPLOYMENT

Dec 2009:
TSA moves FBSs to primary screening

Nov 2012:
Secure 1000 arrives at our lab

2007 2008 2009 2010 2011 2012 2013 2014

Feb 2007:
TSA introduces FBSs as ‘secondary screening’

Dec 2009:
Failed bombing of Transatlantic flight



Rapiscan systems

L3

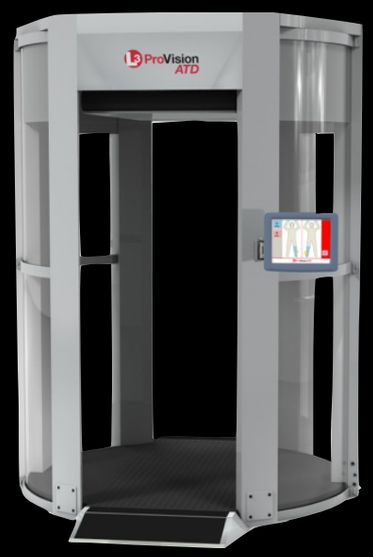



IMAGE: RAPISCAN CORP., L-3 COMMUNICATIONS

# FULL BODY SCANNER DEPLOYMENT

Dec 2009:
TSA moves FBSs to primary screening

Nov 2012:
Secure 1000 arrives at our lab

2007 2008 2009 2010 2011 2012 2013 2014

Feb 2007:
TSA introduces FBSs as ‘secondary screening’

Dec 2009:
Failed bombing of Transatlantic flight







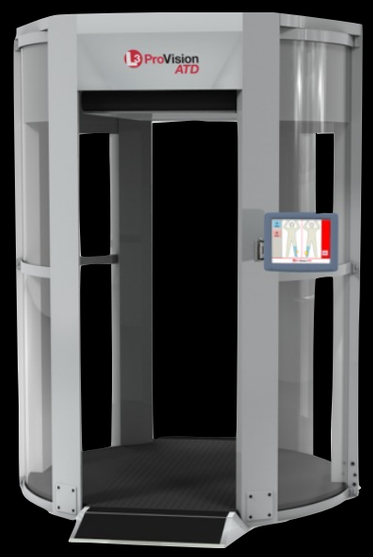



IMAGE: RAPISCAN CORP., L-3 COMMUNICATIONS

# FULL BODY SCANNER DEPLOYMENT

Dec 2009:
TSA moves FBSs to primary screening

Nov 2012:
Secure 1000 arrives at our lab

2007 2008 2009 2010 2011 2012 2013 2014

Feb 2007:
TSA introduces FBSs as ‘secondary screening’

Dec 2009:
Failed bombing of Transatlantic flight

May 2013:
TSA retires Secure 1000







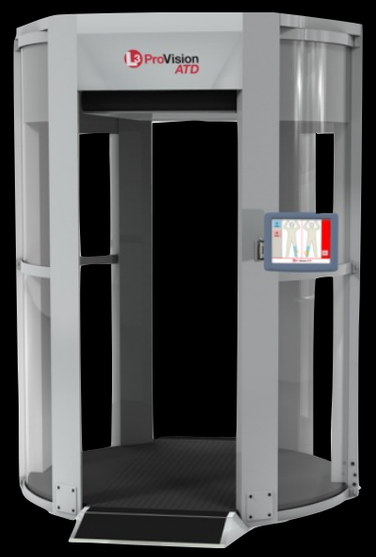



IMAGE: RAPISCAN CORP., L-3 COMMUNICATIONS

# PUBLIC DEBATE

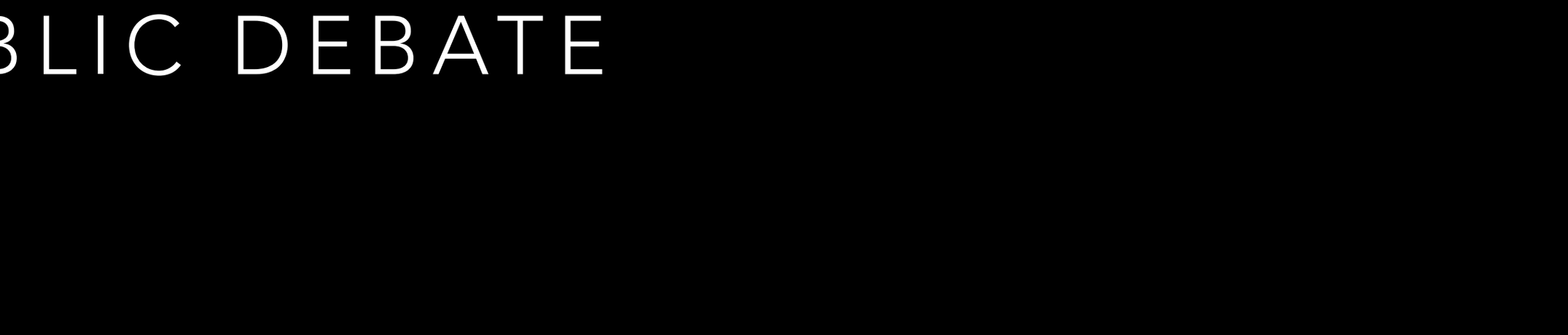
# PUBLIC DEBATE

"... THE DOSE TO THE SKIN MAY BE DANGEROUSLY HIGH."

Radiological Safety? — UCSF University of California San Francisco

# PUBLIC DEBATE

Privacy?




"... THE DOSE TO THE SKIN MAY BE DANGEROUSLY HIGH."

Radiological Safety? – UCSF University of California San Francisco

# PUBLIC DEBATE




Contraband Detection?

Privacy?

the TSO working the NoS said on his headset, "heads up, got a cutie for you."

security at DEN with his 18 year daughter. As his daughter approached the detector, the TSO working the NoS said on his headset, "heads up, got a cutie for you." He then confronted the TSA clerk with what he said and that neither of us are going through the NoS. The TSA clerk said you must have misunderstood me.

He is taking it up with Skywest, with this behavior. Normally, crews there go through a different screening area, but since he was with his daughter, he got to see the TSA clerks at their finest in Denver.

Its stoiries like this, is why I will not go through the NoS (radiation/health issues) and even refuse the the pat-down thus (if it happens while on duty) canceling the flight due to a hostile work environment.

I hope this gets resolves soon!! Got to fly....no NoS checkpoints on this trip so don't worry about a canceled flight from me!!

Quote

"... THE DOSE TO THE SKIN MAY BE DANGEROUSLY HIGH."

Radiological Safety? — UCSF University of California San Francisco

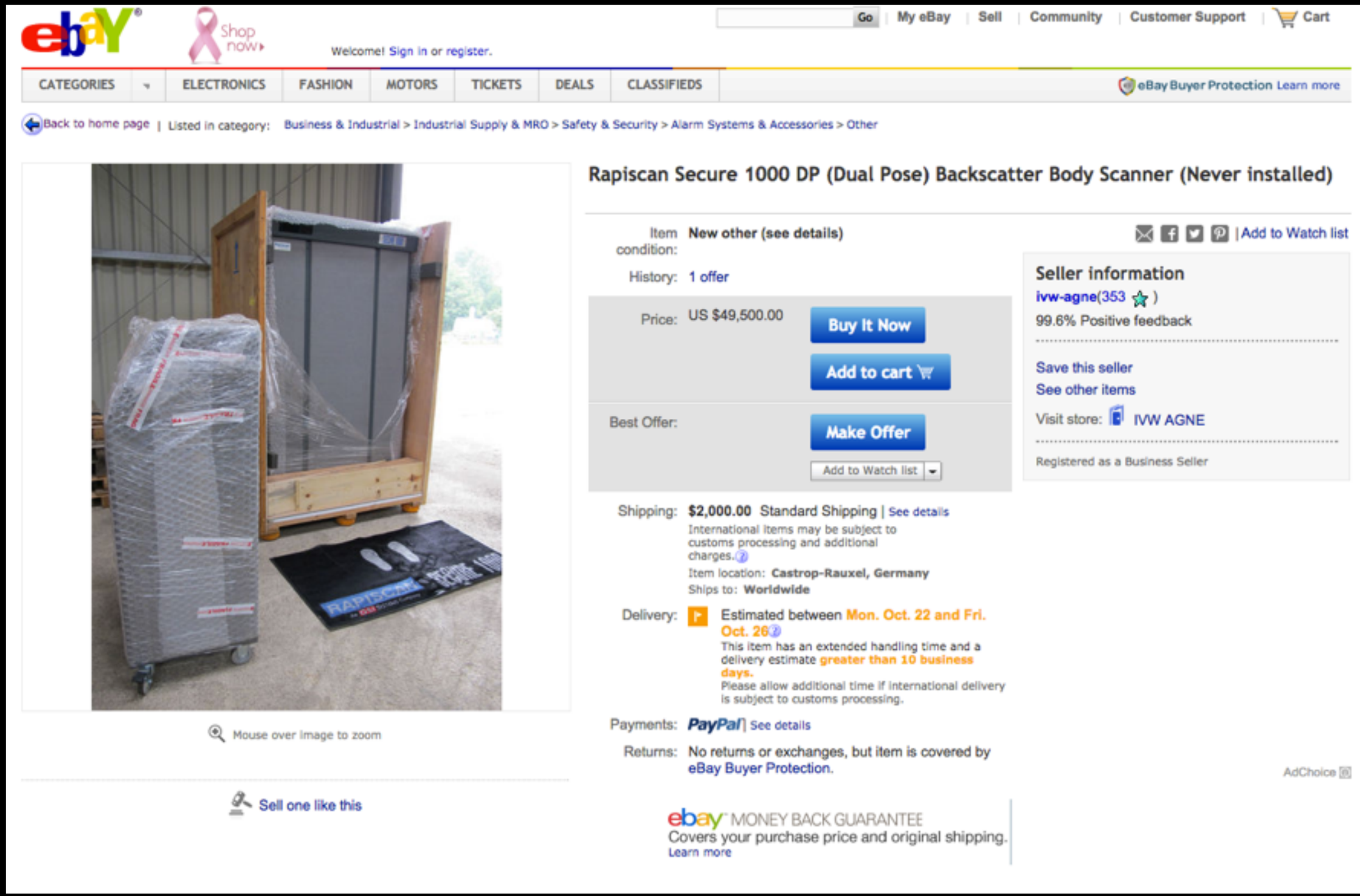
# TSA RESPONSE

Table 8-7 provides the exposure and background readings for the master unit and Table 8-8 provides the readings for the slave unit. Figure 8-10 provides the locations of the readings. As shown in Table 8-7 and 8-8, the dose above the units [redacted] 5 USC 552(b)(4)

that occurs at the beginning of each scan. When the Single Pose system executes a scan, the start position (for the first scan) of the X-ray generator [redacted] When the scan is initiated, the X-ray generator (and therefore x-ray beam) [redacted] Therefore, the primary beam points toward [redacted]

[redacted] During this phase [redacted] are not monitored because as they are out of tolerance. [redacted] At this time it is assumed that [redacted] and these parameters are monitored. Therefore, there is approximately 0.5 seconds at the beginning of each scan where vertical motion has not reached peak velocity and may result in slightly higher doses at the position where the scan starts.

# ACQUISITION



# OUR CONTRIBUTION: THE FACTS

1. Is the Secure 1000 radiologically **safe**?

2. What **privacy** safeguards exist?

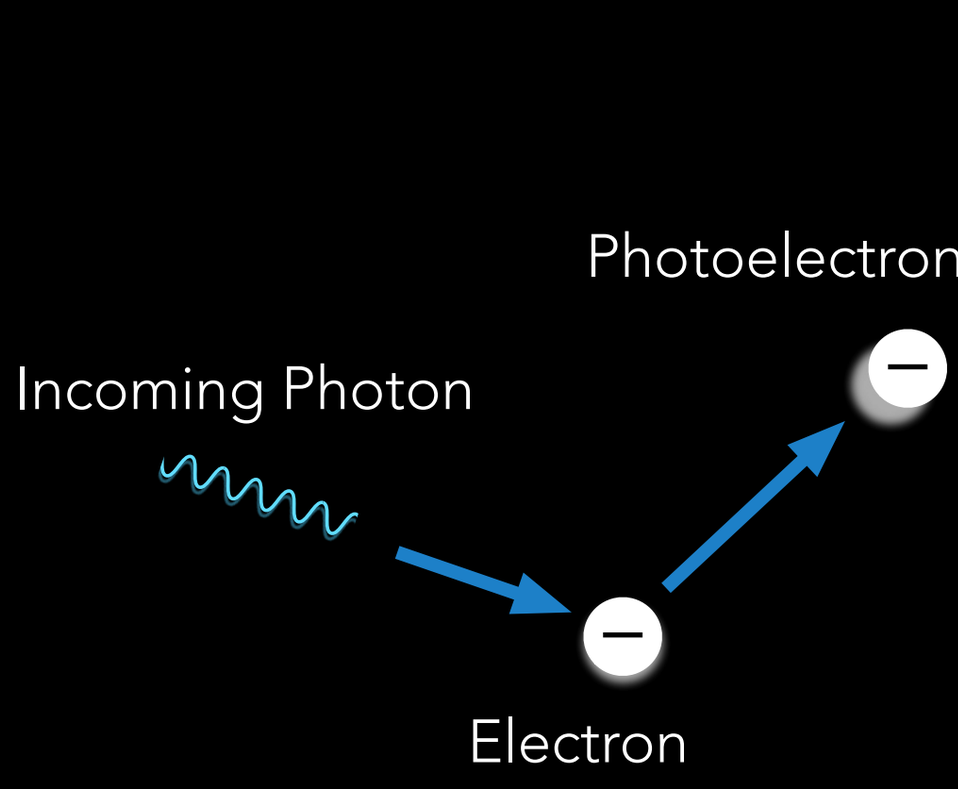
3. How **effective** is it at detecting contraband?

Cyberphysical systems use software!

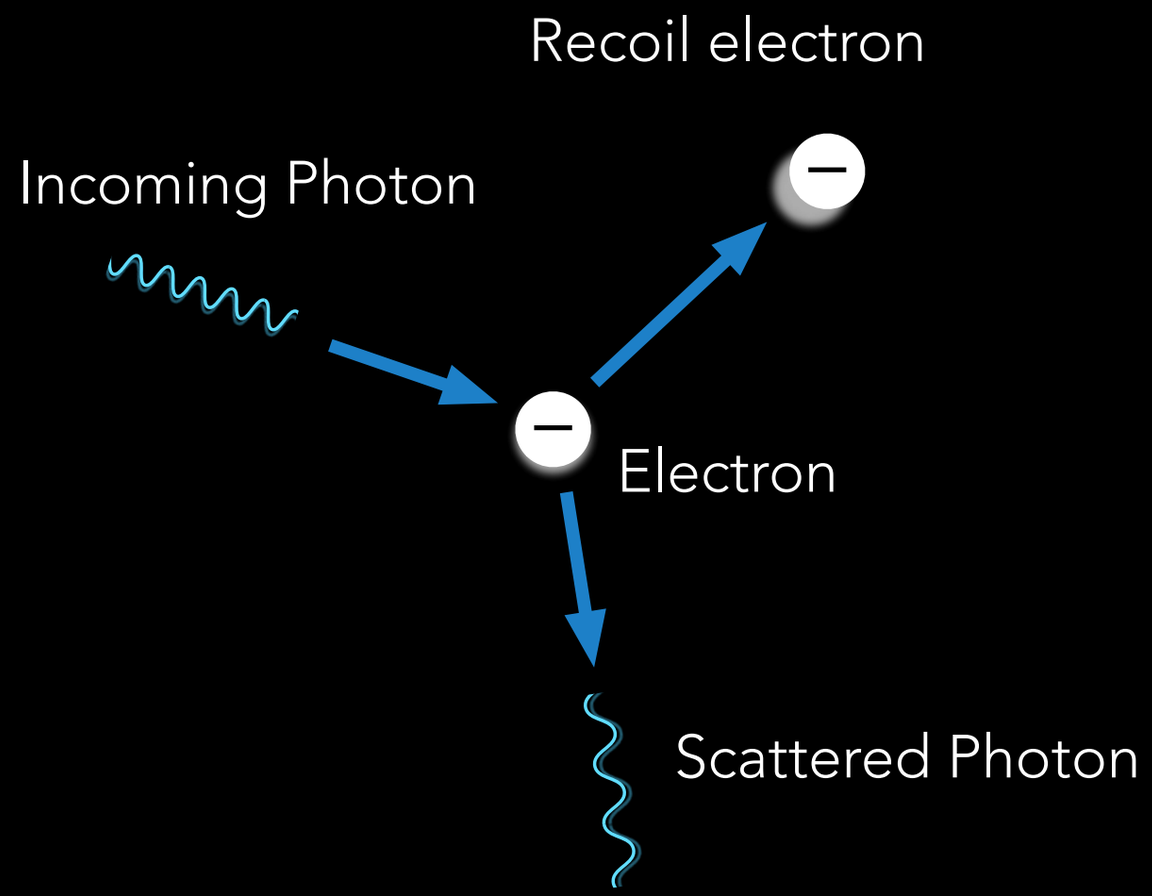
# INSIDE THE SECURE 1000



# X-RAY PHYSICS 101



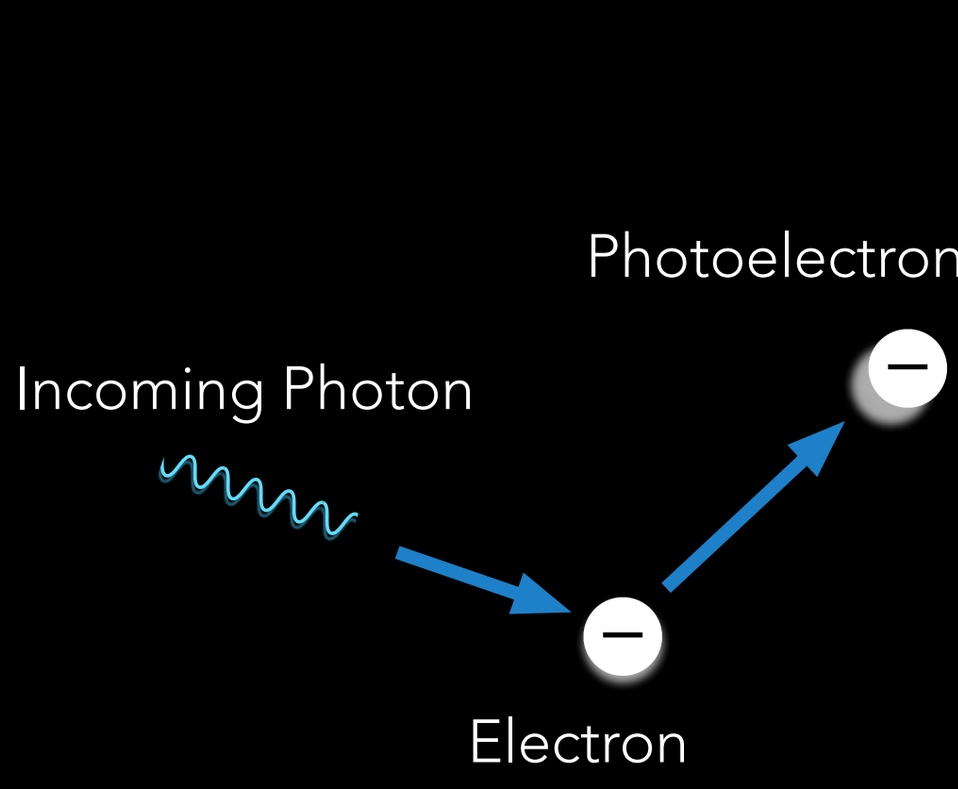

Photoelectric Effect



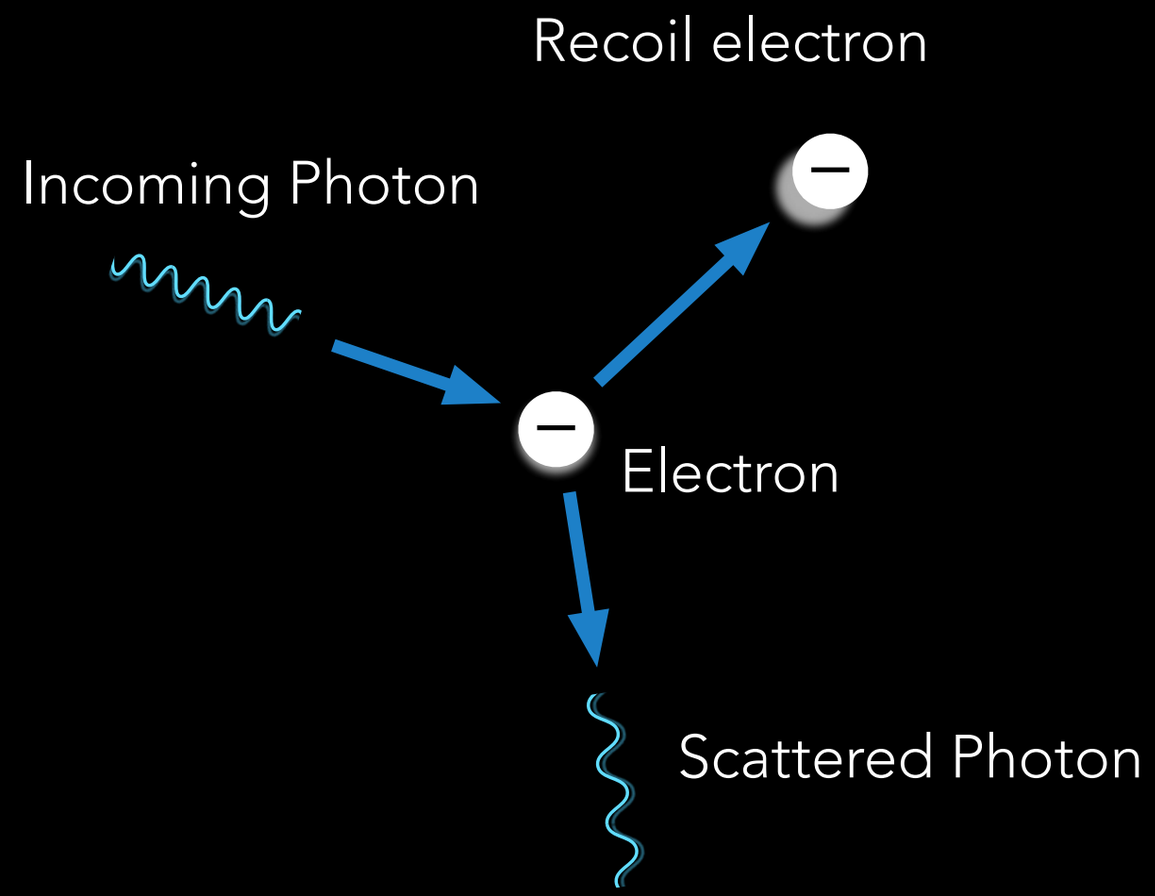

Compton Scattering

Low energy X-ray: 50 KeV at 5 mA

# X-RAY PHYSICS 101




Photoelectric Effect




Compton Scattering

Dominant effect depends on material's "effective atomic number"

# SECURE 1000 X-RAY HARDWARE

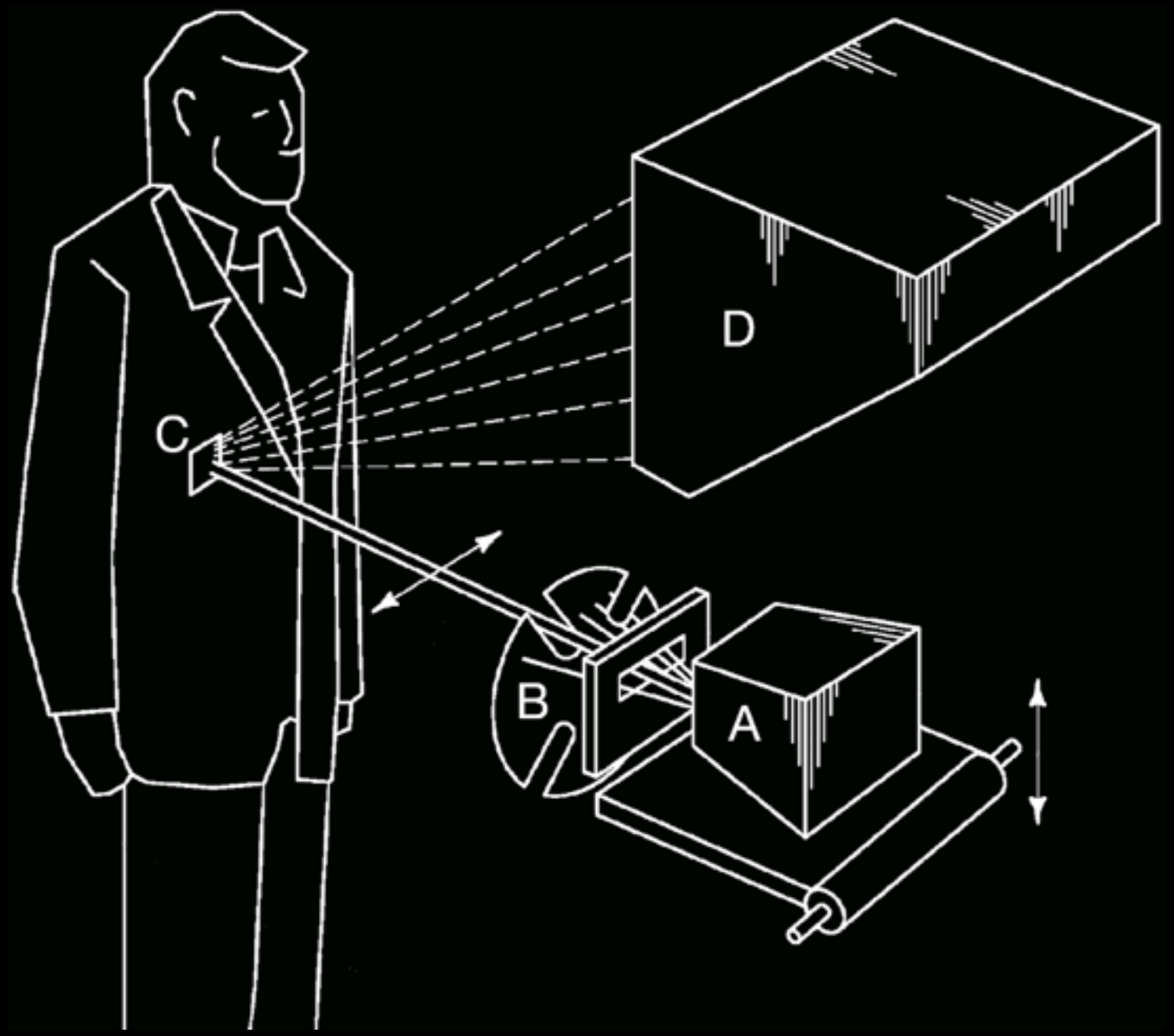



FIGURE ADAPTED FROM U.S. PATENT 8,199,996
R. HUGHES, JUNE 2012

# SECURE 1000

- Chopper spins
- Head assembly moves vertically



# SECURE 1000

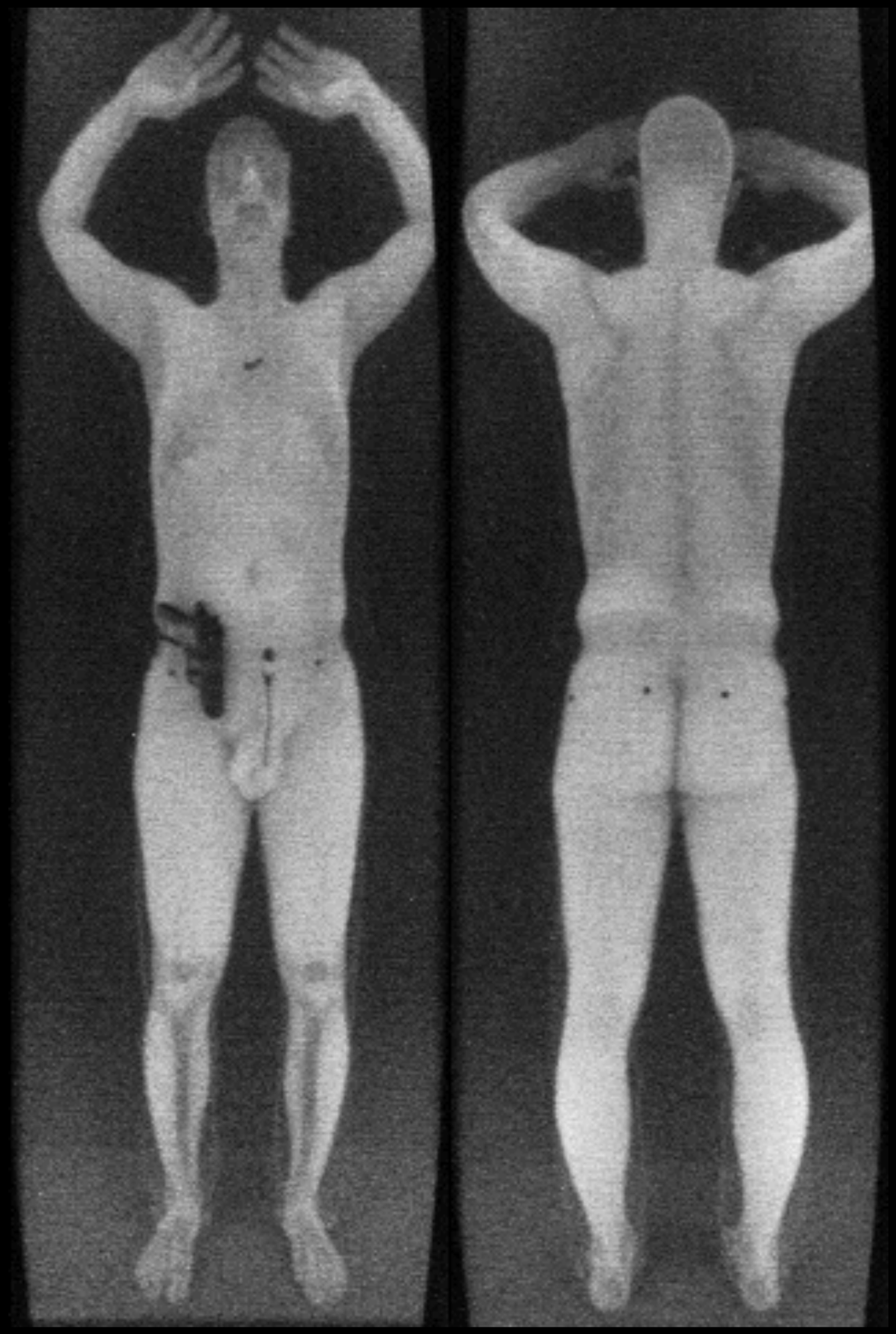
- Chopper spins
- Head assembly moves vertically



# SECURE 1000 X-RAY HARDWARE



# IMAGE PRODUCTION



# OUR RESULTS

# RADIATION SAFETY



# RADIATION SAFETY

- X-ray energy: 50 KeV at 5 mA
- Dose per scan: 70-80 nSv
  - ~24 minutes of background exposure
  - Similar results by AAPM (2013)



# CYBERPHYSICAL RADIATION SAFETY

- Safety controls on radiological output
  - Not security controls!
- Simple, modular design
  - Cannot over-irradiate scan subject without ROM replacement

# OPERATOR SOFTWARE



SECURE 1000™ personnel screening system
Rapiscan Security Products, Hawthorne, CA
FOR USE BY QUALIFIED OPERATORS ONLY

scan
zoom
clear
redraw
→ save
recall
comments
options

Press ENTER to save images to the harddisk.

Press the ↑↓ keys to select another action.

08-14-14 11:16

# CONSOLE MALWARE



"Secret knock"



Visible light



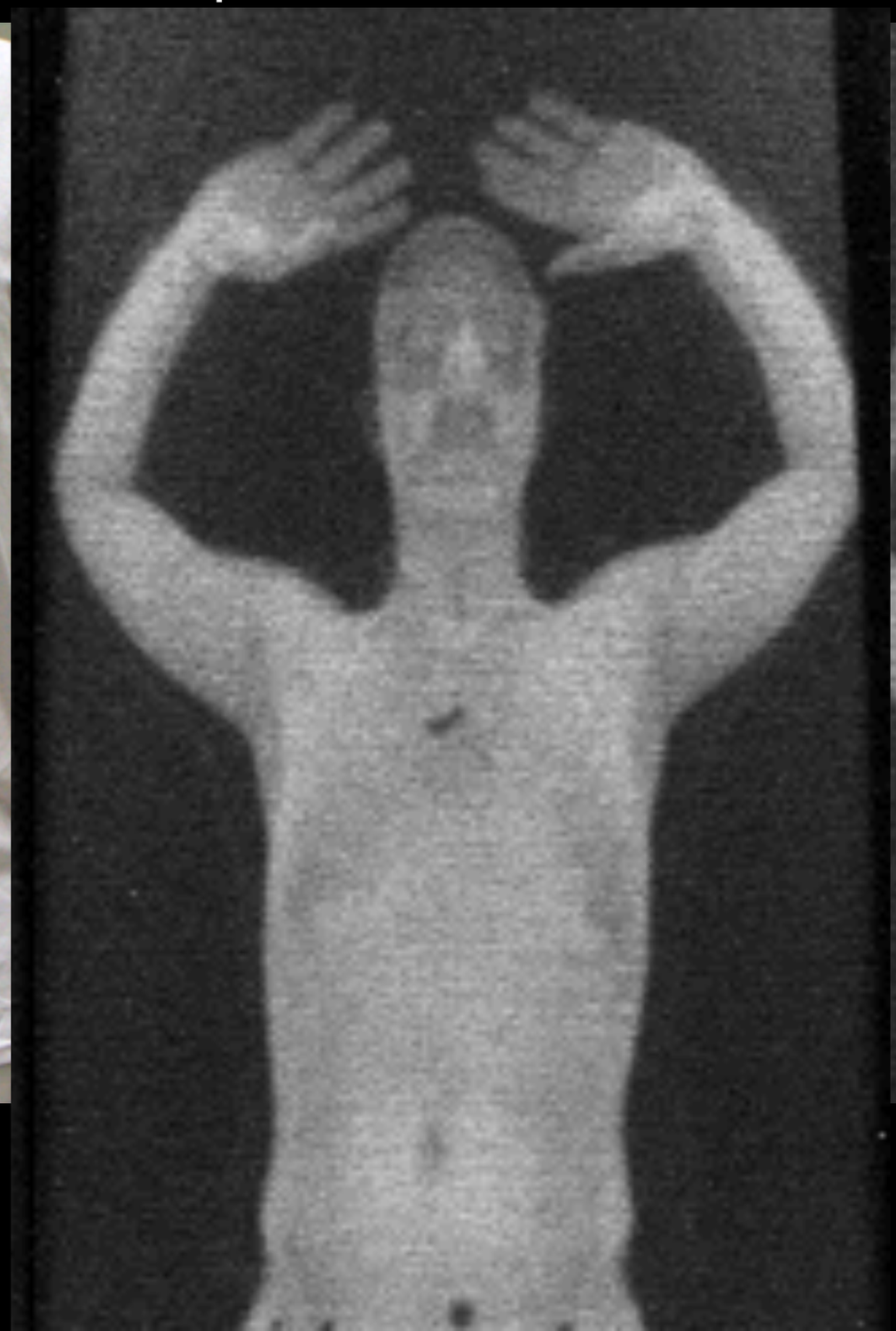
X-ray

# CONSOLE MALWARE

## Operator's View



"Secret knock"



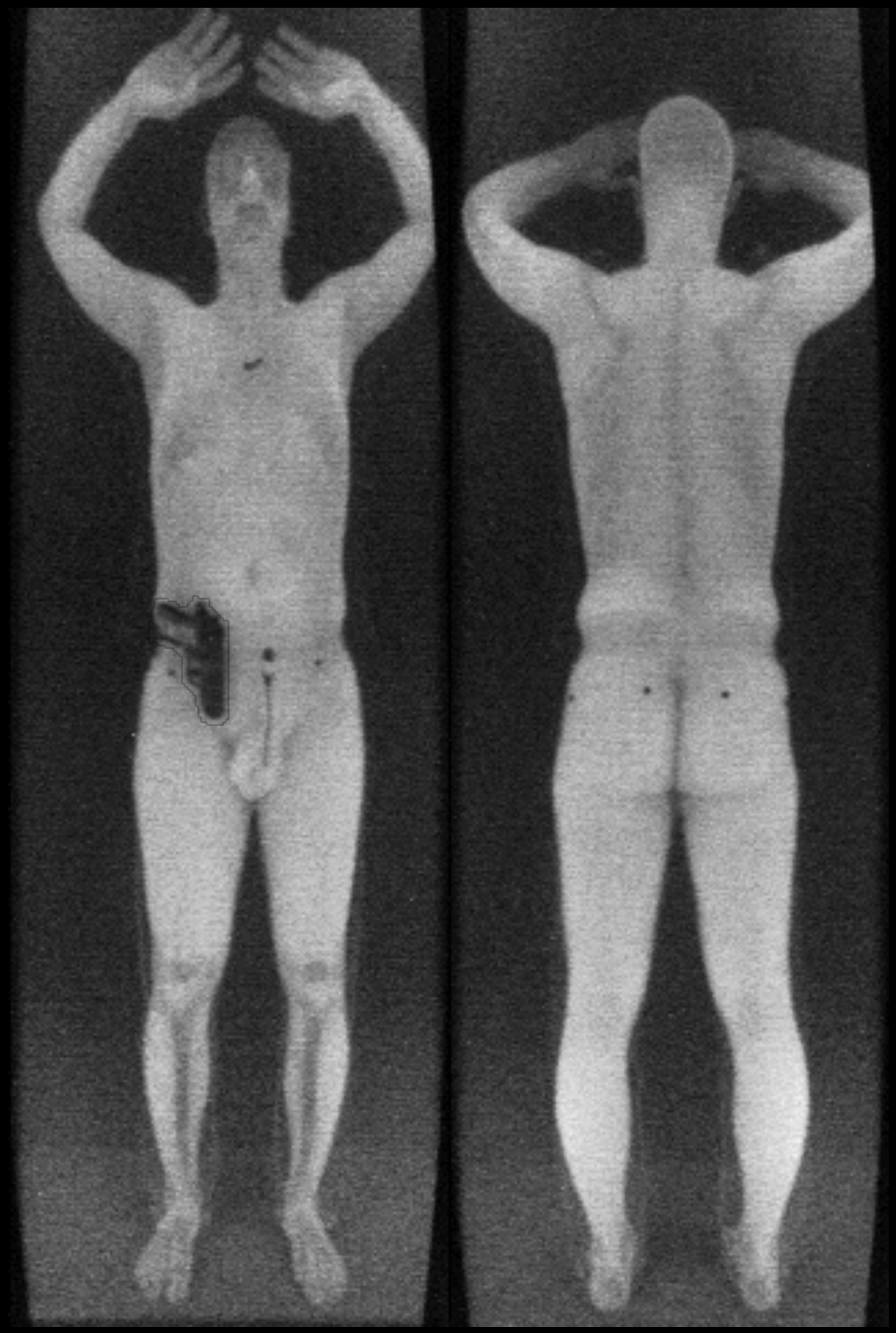


X-ray

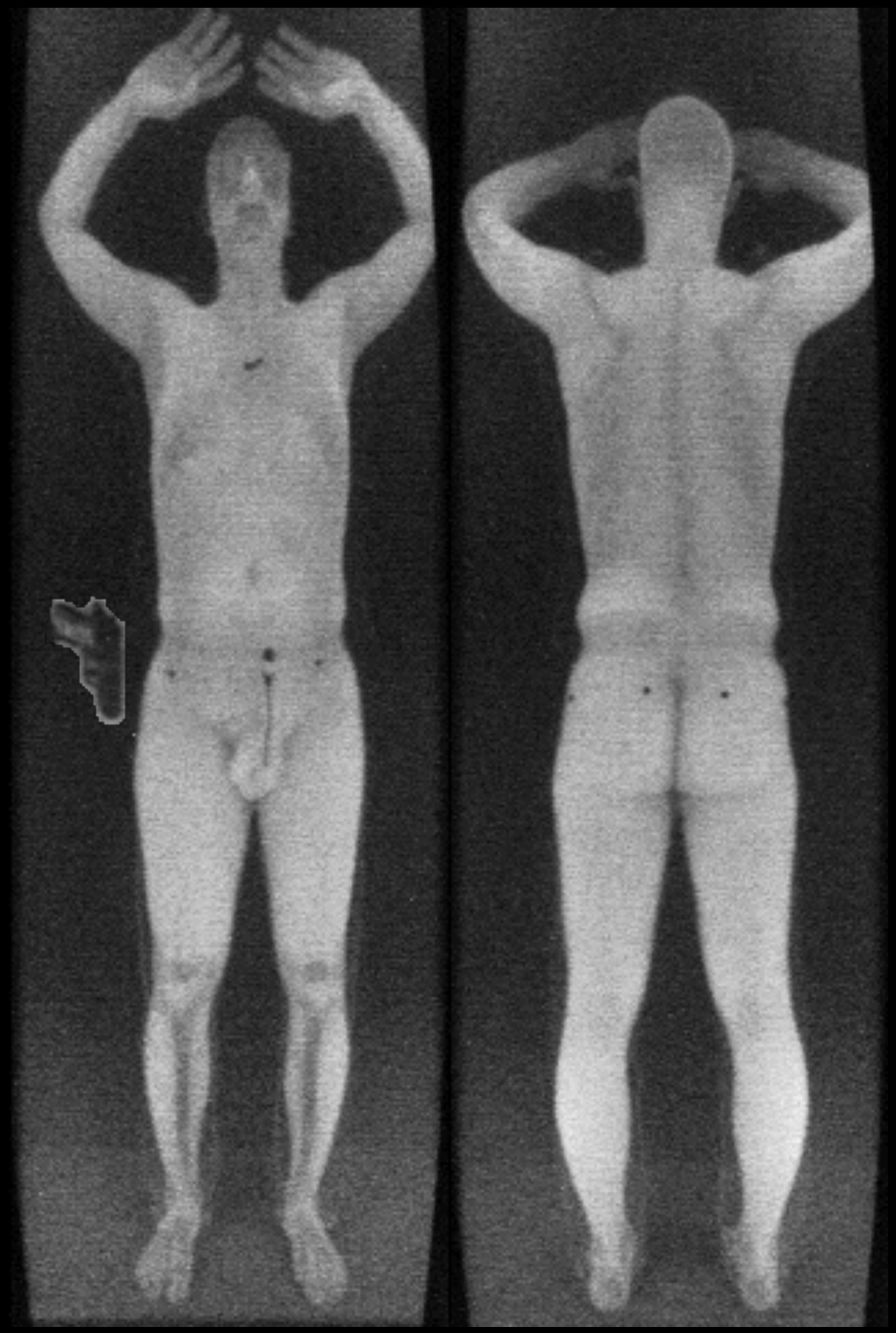
# HANDS-OFF ATTACKS



# ADVERSARIAL PHYSICS



# ADVERSARIAL PHYSICS



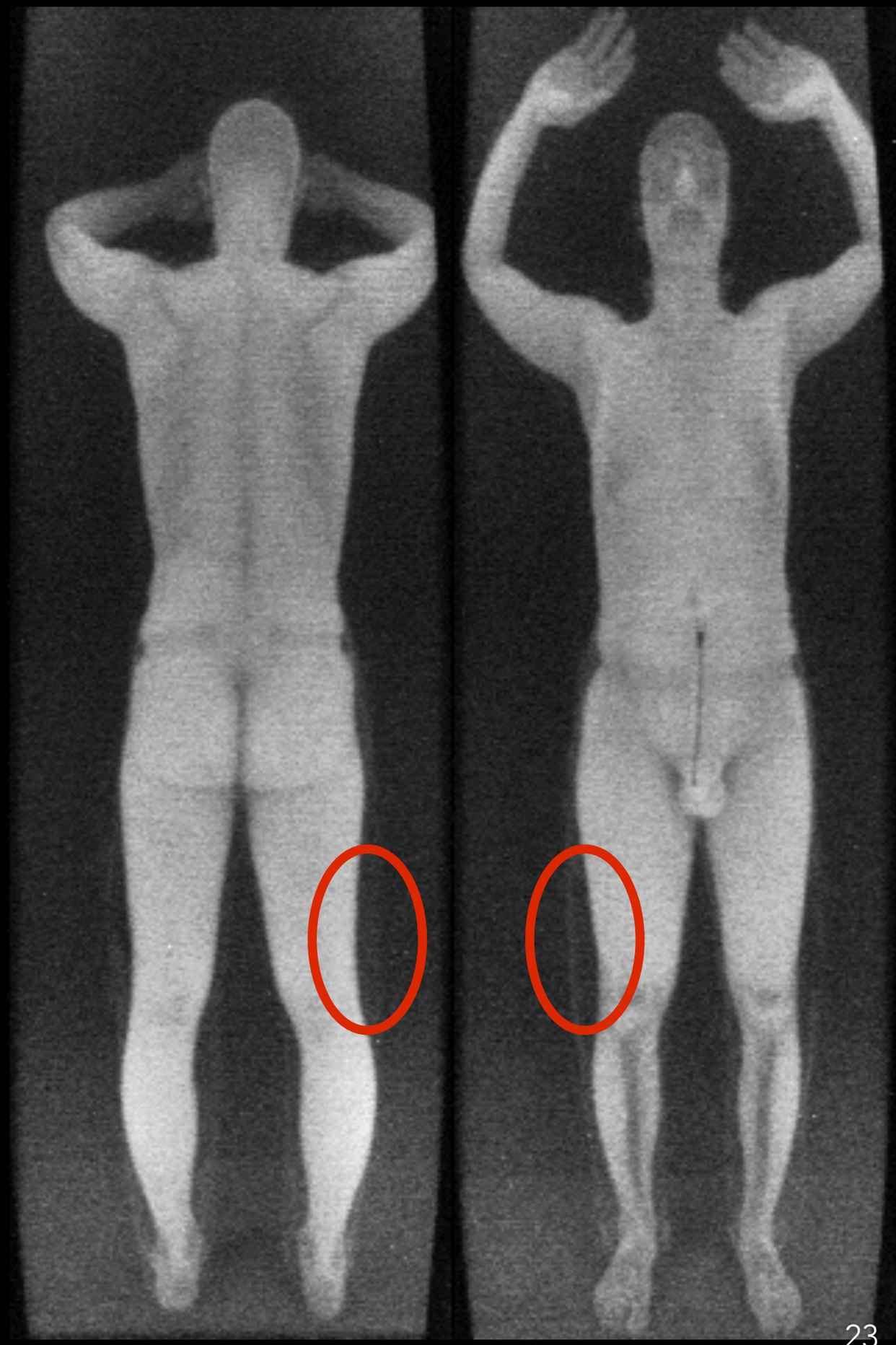
# FIREARMS

- Subject is carrying a .380 ACP pistol



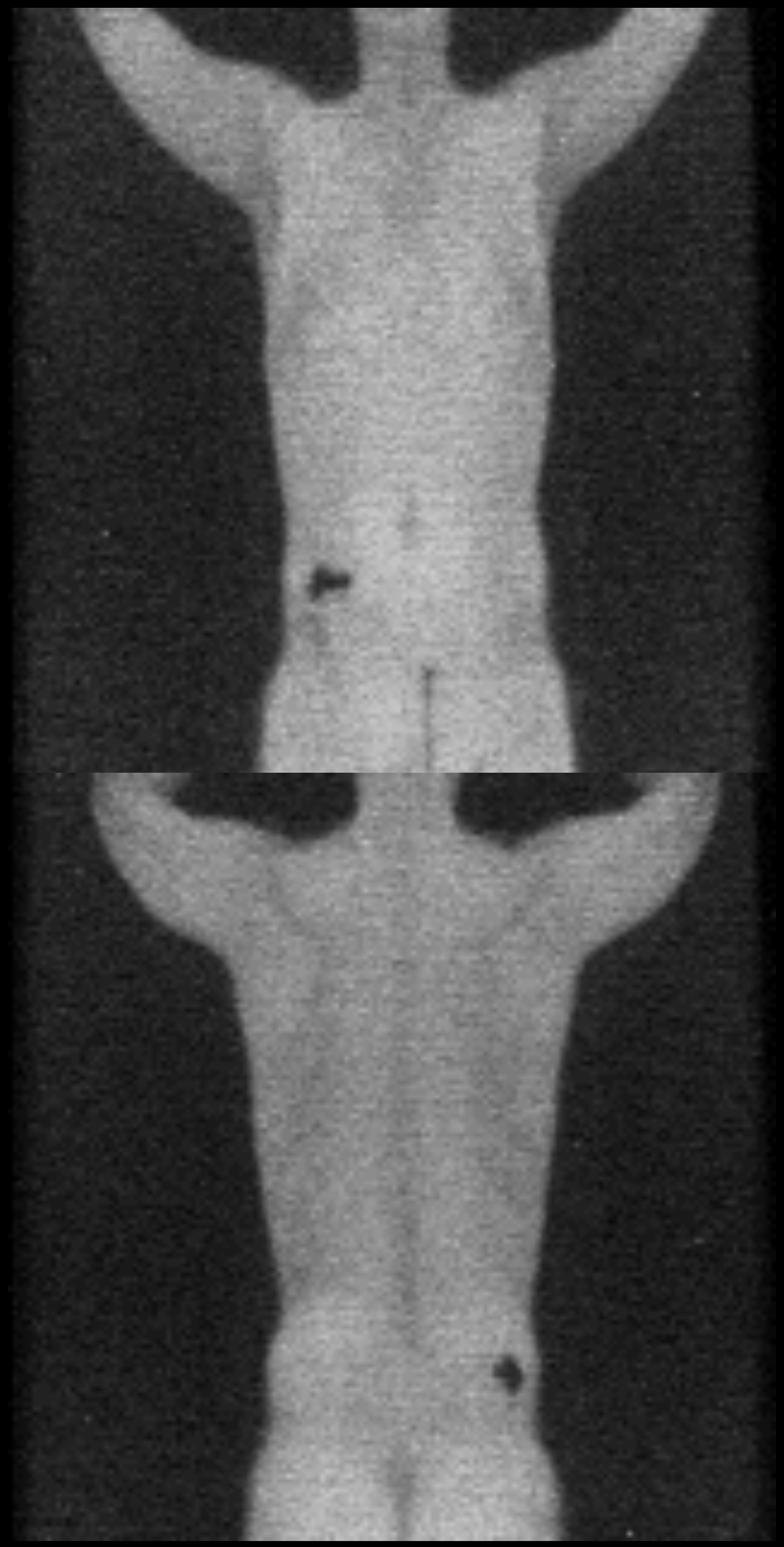
# FIREARMS

- Subject is carrying a .380 ACP pistol



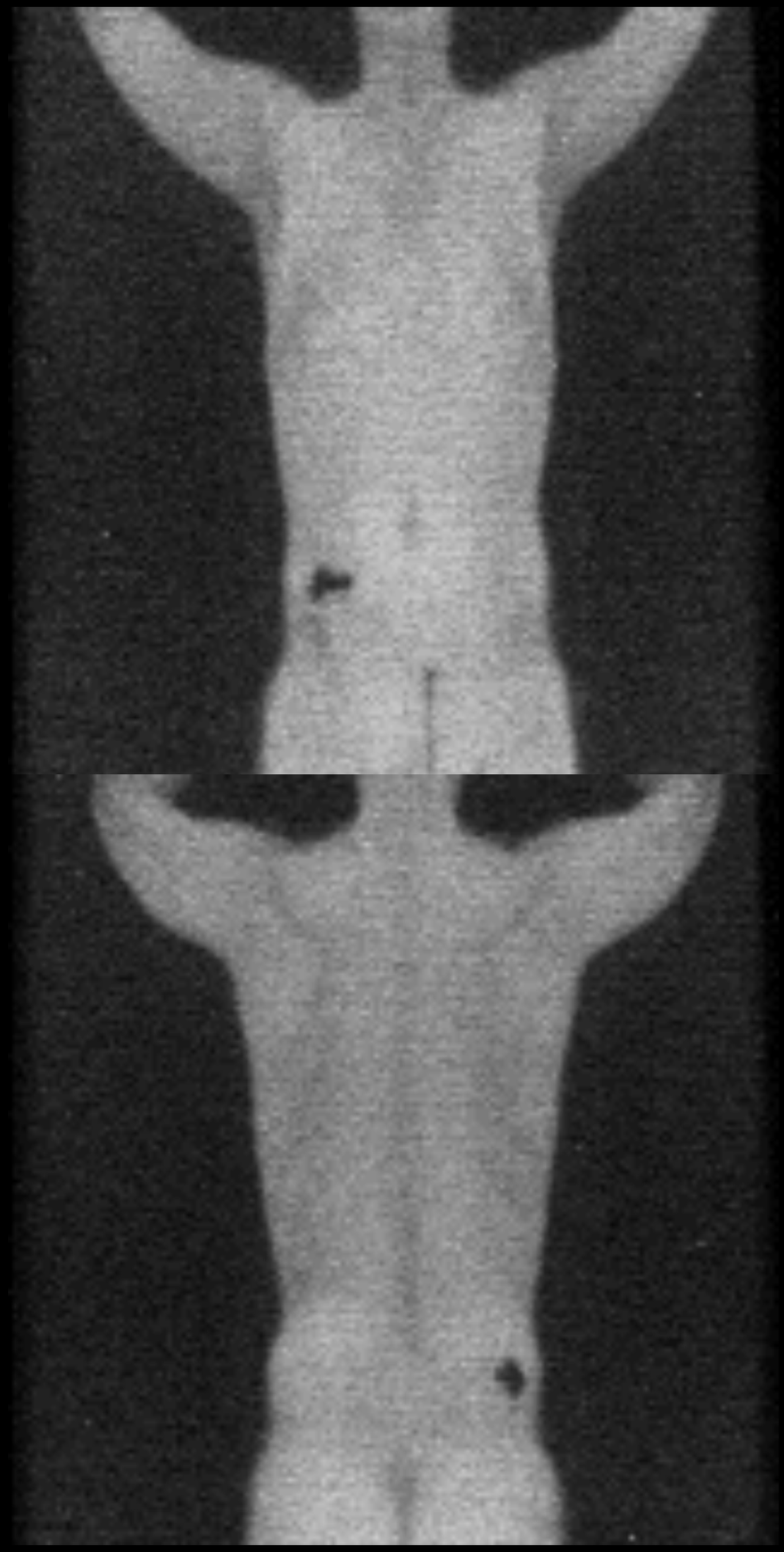
# FOLDING KNIFE

- Subject is carrying a folding knife



# FOLDING KNIFE





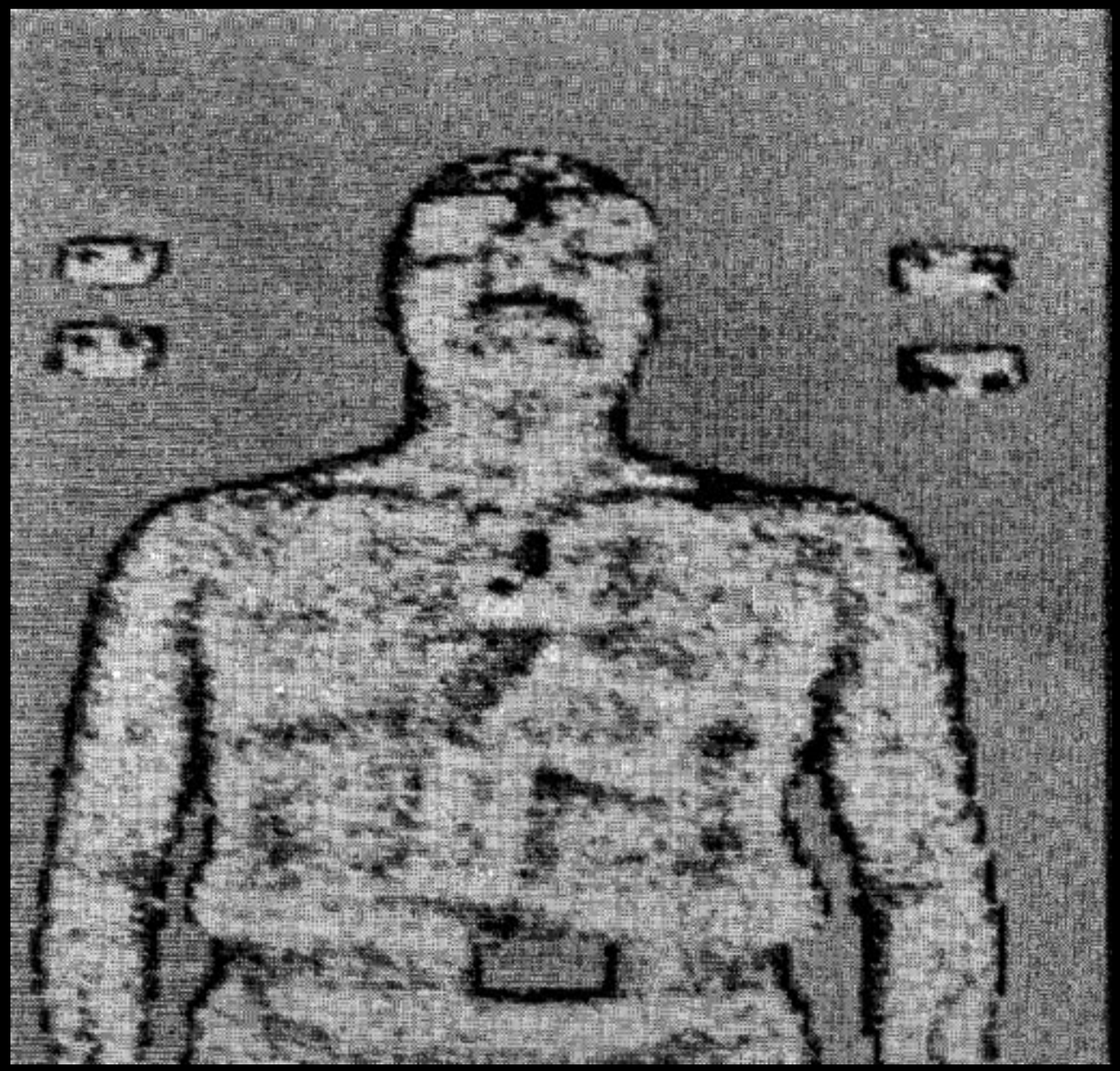
# PLASTIC EXPLOSIVES



After the failed Christmas Day "underwear bombing" attempt in 2009, Napolitano launched a worldwide and "historic" effort — in 190 countries — to enhance passenger screening and counter the threat of "nonmetallic devices" on aircraft, she said.

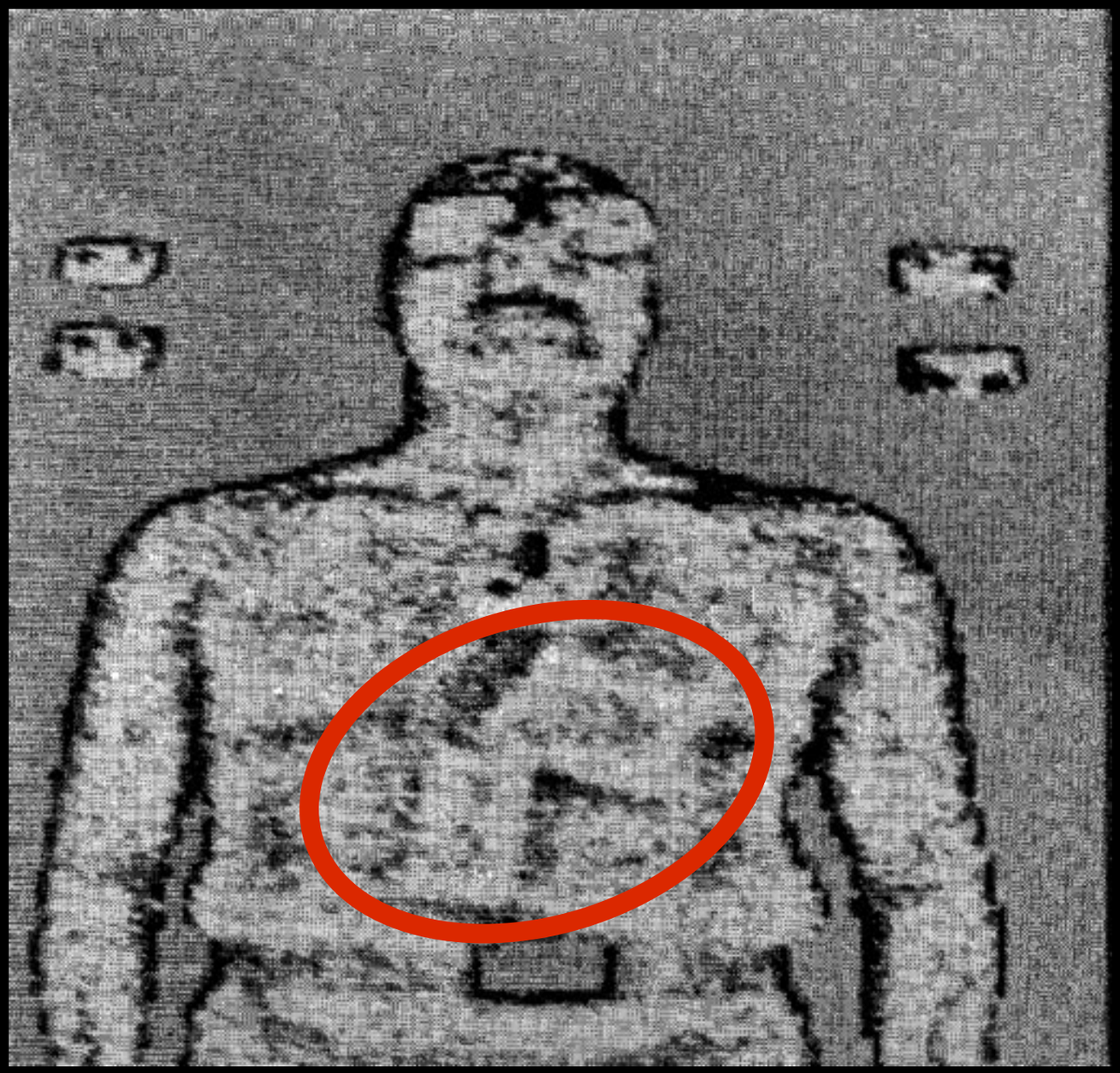
QUOTE: HTTP://ABCNEWS.GO.COM/BLOGS/POLITICS/2013/08/OUTGOING-DHS-SECRETARY-JANET-NAPOLITANO-WARNS-OF-SERIOUS-CYBER-ATTACKUNPRECEDENTED-NATURAL-DISASTER/

# SANDIA: C4 DETECTION (1992)



REPRODUCED FROM "EVALUATION TESTS OF THE SECURE 1000 SCANNING SYSTEM"
TECHNICAL REPORT SAND 91-2488, UC-830, SANDIA NATIONAL LABORATORIES, APR. 1992.

# SANDIA: C4 DETECTION (1992)



REPRODUCED FROM "EVALUATION TESTS OF THE SECURE 1000 SCANNING SYSTEM"
TECHNICAL REPORT SAND 91-2488, UC-830, SANDIA NATIONAL LABORATORIES, APR. 1992.

# THINK ADVERSARIALLY!



# THINK ADVERSARIALLY!





Plastic!

# PLASTIC EXPLOSIVES

Subject carrying 200+ g of C-4 simulant

vs.

No contraband

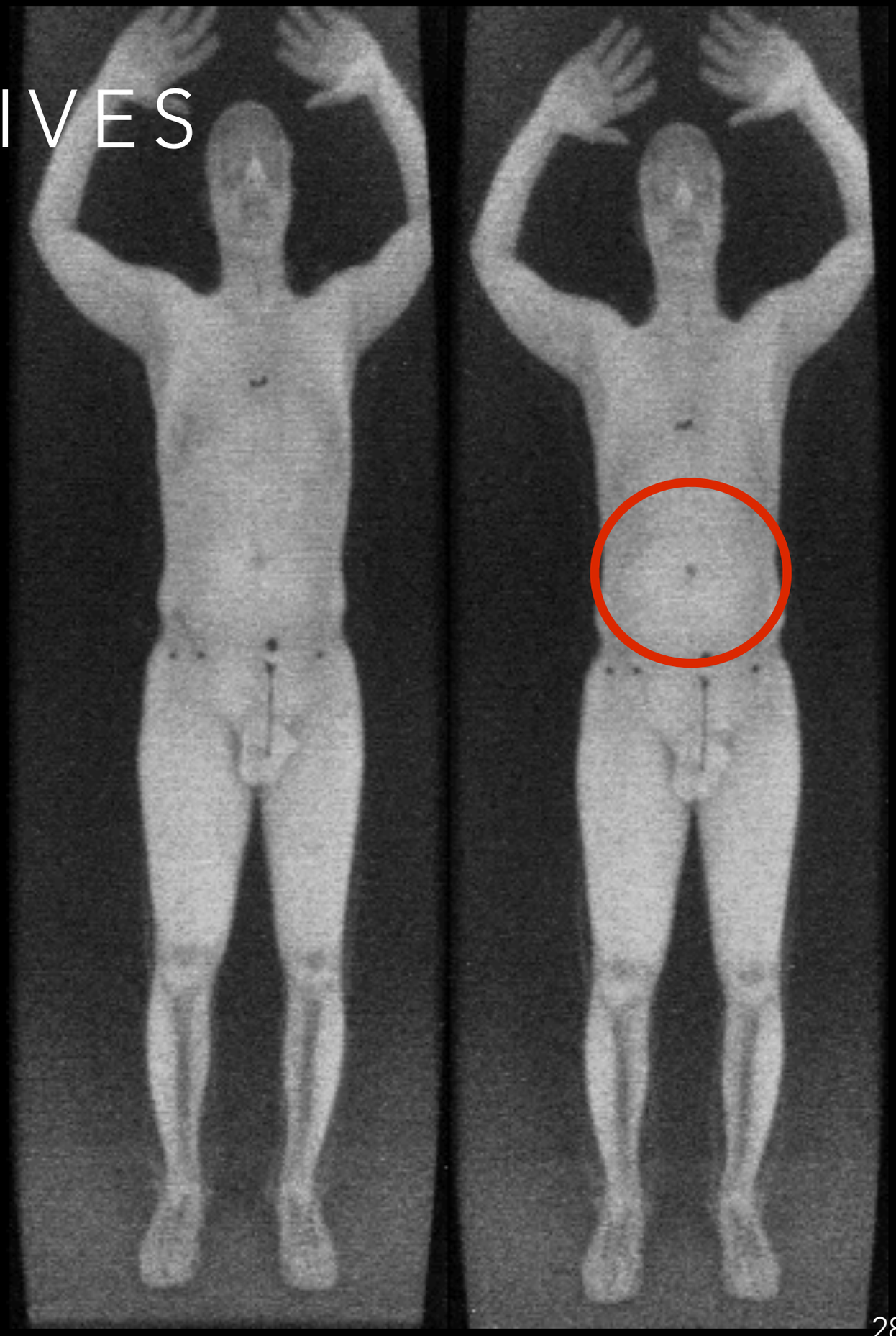


# PLASTIC EXPLOSIVES

Subject carrying 200+ g of C-4 simulant

vs.

No contraband

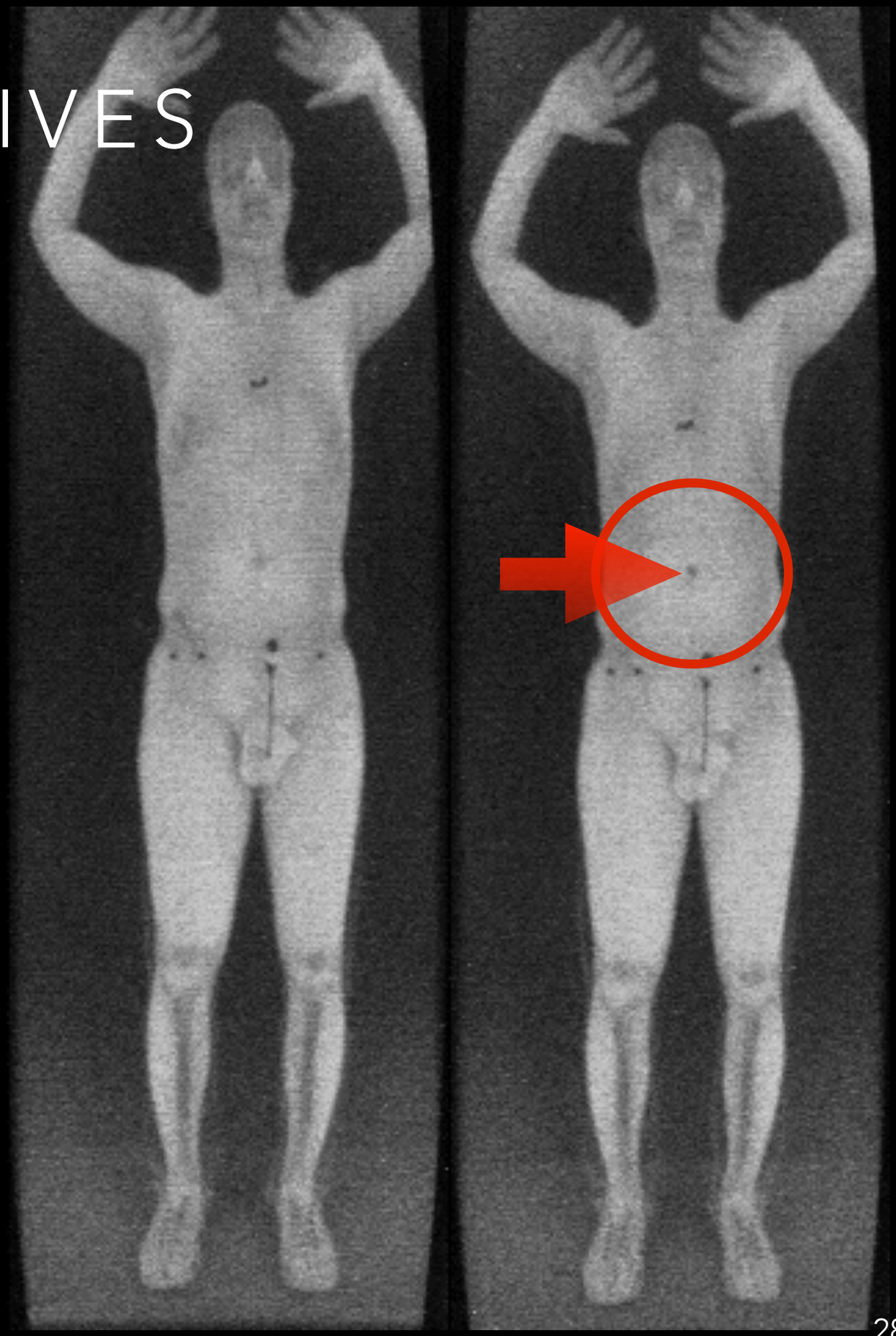


# PLASTIC EXPLOSIVES

Subject carrying
200+ g of C-4
simulant

vs.

No contraband



# EFFICACY RESULTS

- Our results imply adversaries can conceal:
  - Knives
  - Firearms
  - Plastic Explosive & Detonators

- Access to Secure 1000 allows attack refinement

# DISCUSSION AND LESSONS

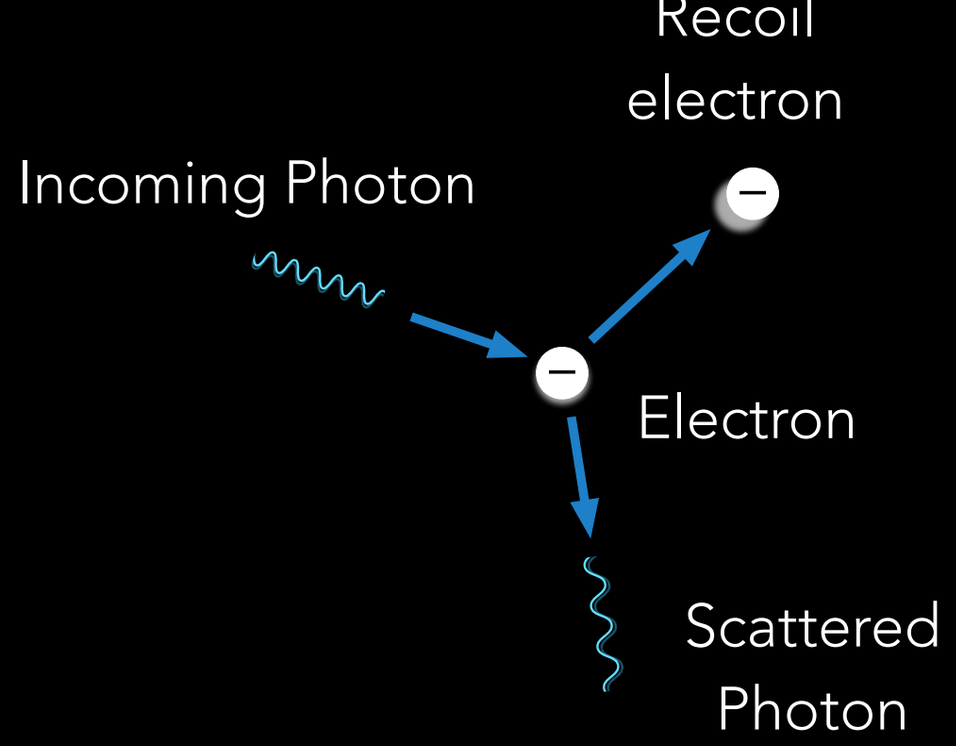
# POLICY IMPLICATIONS

- Secure 1000 used at airports despite major flaws
  - Either TSA didn't know (inadequate testing) or didn't act

- Critical security infrastructure needs independent, rigorous, transparent testing
  - Including cyberphysical security testing!
  - Apply adaptive adversarial thinking

# LESSONS FOR DEVELOPERS

- Simple, modular design
  - Remote malicious X-ray emittance not possible in Secure 1000
- Physics matters
- But only if software is safe!
  - Compromised software -> complete security failure



# MITIGATIONS

- Disclosed results to DHS and Rapiscan in May 2014



- Procedural mitigations
  - Perform side scans
  - Pair with metal detectors

# ADVANCED IMAGING TECHNOLOGY: TODAY & TOMORROW

- AIT deployed at nearly 160 U.S. airports
  - L-3 ProVision (millimeter wave)
  - Automated Threat Recognition
- TSA testing new X-ray backscatter AIT

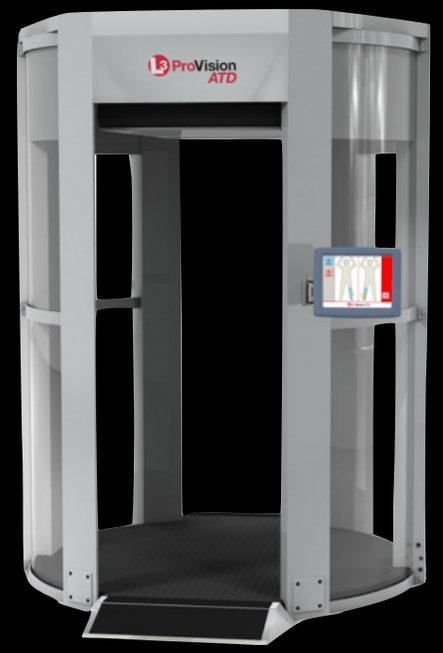





IMAGE: L-3 COMMUNICATIONS, AMERICAN SCIENCE & ENGINEERING

# SECURITY ANALYSIS OF A FULL-BODY SCANNER

KEATON MOWERY, ERIC WUSTROW,
TOM WYPYCH, COREY SINGLETON,
CHRIS COMFORT, ERIC RESCORLA,
STEPHEN CHECKOWAY,
J. ALEX HALDERMAN,
HOVAV SHACHAM

Questions?

More information at
https://radsec.org

