“Algorithmic Transparency and Emerging Privacy Issues”
Marc Rotenberg, EPIC
UNESCO
Paris, France
2 December 2015

“At the core of modern privacy law is a single goal: to make transparent the automated decisions that impact our lives.”

“Fundamental Rights include principles of procedural fairness and transparency”
“As decisions are automated, processes become more opaque, less accountable.”

“Even large, powerful organizations, such as the National Security Agency (NSA), do not fully understand the systems they are building”

“We need a new way to talk about ‘Internet policy,’ one that builds on familiar paradigms, but is more far-reaching and more forward-looking”
The New Paradigm: “Algorithmic Transparency”

- Next Stage in Development of Transparency Law
  - FOIA / Right to Information -> “Open Data” -> “Algorithmic Transparency”
- Next Stage in Development of Internet Law
  - “Open Internet” -> “Algorithmic Transparency”
- Next Stage in Development of Privacy Law
  - “Fair Information Practices” -> “Algorithmic Transparency”

“At the intersection of law and technology — knowledge of the algorithm is a fundamental right, a human right”

Related Work on Algorithmic Transparency

- Frank Pasquale - *Black Box Society* (2015)
- Gary Marx - “Block modelling” (1983)
- Willis Ware - “Records, Computers, and the Rights of Citizens” (1973)

Current EPIC Cases

- EPIC Files Lawsuit For Details of Government Profiling System” (2014)
- “EPIC Objects to Secret Profiling of Air Travelers” (2013)
- “Student Privacy Bill of Rights calls for algorithmic transparency” (2013)
Next Steps - EPIC 2015

- Program Development
- Litigation
- Public Campaign
- Academic Outreach
- Purposeful - Seek Constructive Outcome

EPIC v. DHS. Not a Movie. EPIC is seeking documents about Homeland Security's plans for "pre-crime detection." Tom Cruise starred in a 2002 movie about "a special police unit that is able to arrest murderers before they commit their crime."

Other Emerging Privacy Issues
• Tracking of vessels (EPIC v. US Coast Guard)
• Surveillance by drones (EPIC v. Federal Aviation Administration)
• Connected vehicles and “Internet of Things” - privacy and public safety concerns
• Transborder data flows after the Schrems decision
• (Consult epic.org for more information)
• One more big idea - - -

Themes

• Claims of privacy are also claims about the ability of the individual to control disclosure of identity
• Anonymity protects privacy and freedom of expression
• Anonymity is a right of natural persons
• “Initiatives to protect privacy and anonymity online” (UNESCO 2014)
• But accountability is needed for machines, and autonomous devices (drones, robots)
Consequences

- Need for accountability for autonomous devices
- Example #1: people may act anonymously - machines may not
- Example #2: people may speak anonymously - machines may not
- Example #3: people may keep secrets - machines may not

Asimov, “Law of Robotics”

(Handbook of Robotics, 56th Edition, 2058 A.D.)

- “A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.”
- “A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.”
- “A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.”
- NEW - “A robot must always reveal to a human being the basis of its decision.” (Algorithmic Transparency)