Naked Crowd

By Jeffrey Rossen
Motivation For the Book

- Lawrence Lessig who teaches at Stanford Law School challenged Jeffrey to respond with solutions to design technology and regulate laws that will protect Liberty and security at the same time.
- Case Study: Proliferation of Cameras in Britain
Introduction

- After 9/11 the testing of the Naked Machine (a new security device) started at Orlando International Airport.
- It was an electronic strip search which used microwaves and millimeter waves to create a 3D naked image of everyone it scrutinizes.
- Unlike conventional metal detectors common at most airports today this machine could detect plastic and even ceramic concealed within clothes.
- A price to pay in this age of terror.
• This technology demanded high level of security.
• Could be used at all public places not only airports.
• This machine demanded high sacrifice of liberty and privacy!
• Everyone who passed under this new scanner exposed themselves nakedly even if they posed no threat and were not concealing anything.
Solution to this threat:

- Researchers at the Pacific Northwest National Laboratory in Washington State with a simple programming shift redesigned the Naked machine which now showed them concealed objects projected on a sexless mannequin.
- In simple terms the lurking image of a naked body were scrambled into an unrecognizable blob.
- The redesigned version of the Naked machine was thus named as the blob machine.
This new Machine guaranteed exactly the same amount of privacy without having to invade Liberty and Privacy.

For all protectors of privacy and liberty the choice between The Naked Machine and the Blob Machine was simple.

But when a survey was taken among students and adults post 9/11 a surprisingly large number of people say that they would rather go through naked machine than the blob!!! Reasons:

- Lost hope and fed up anyways.
- Not embarrassed
- Nothing to hide, nothing to fear argument
Most of the public opinion about which security system to standardize was not important.

The public was more concerned with feeling safe rather than being safe.

Despite the fact that both these machines gave the same outcome an important strain of public opinion preferred to go through the naked machine so as to demonstrate their purity.

This crowd was a part of people who personalized the risk and exaggerate the probability of its occurrence that they felt that security weighed far above trivial matters of liberty and privacy.
Synopticon vs Omnipticon
Chapter One: A Cautionary Tale

Post 9/11 ----- “A new and Anxious Age ”

- Visionics - A New Jersey Company with products like Facelt.
- CCTV became the “single most heavily funded non-criminal justice crime prevention measure”
- Warning signs became a common sight:
  - CCTV in Operation
  - CCTV: Watching for You!
  - Smile for the Camera

The cameras lost its original purpose as they slowly started using these cameras for reasons other than finding terrorists!!
CCTV’s in London were now being used for
a. Traffic Updates
b. Stolen Car recognition by scanning license plates
c. Keeping Bad guys from Shopping malls.

“The Face recognition system in England was running for around 3 years now and not a single arrest was made.” - Bob Lack (Former London Police)

There was no clear written standard on who enters the database.

Police did not seem to care who was in the database as these cameras were more of a deterrent to crimes in areas of public space.

It was more safe for the public to believe that all of them were in scrutiny and being watched in order for them to feel safe.
The problem with so many cameras was that there were not many people behind those screens to monitor them all. The solution was to have surveillance systems that were going to be monitored by face recognition algorithms which would match every face of an individual with homeland security database and send an alert to the authorities whenever a match is found.

In the above case, we would truly get an open society, but this does not mean a transparent society, where everyone can see with a laptop and joystick every detail about the lives of other individuals.

The need is to have a society where everyone redefine and reinvent themselves every day. Travel place to place without being categorized by our past deeds.

In short “Identity of a person will not be limited to a profile in a database.”
Chapter Two: The Psychology of Fear

- Goiânia, Brazil Case study.
- Dramatically branded in the public mind with the stigma of contamination.
- Media hype to create panic disproportionate to the actual threat.
- This chapter deals with how the public reacts to emotional fear rather than analytical sound fear.
- Public fear is the most important barrier to efforts to design laws and technologies that protect liberty and security at the same time.
- This fear makes the public accept or embrace technology that threatens privacy and liberty without increasing security.
- Paul Slovic of the University of Oregon says that public is influenced with images of threats more than the arguments.
The law of contagion

1. Fear of anthrax leads to a 5 billion dollar loss (2001)
2. Reactions were as follows:
   a. Hart Senate Office Building was closed for months and decontaminated at a cost of $22 million.
   b. FBI investigated 2,500 reports of suspected anthrax attacks
   c. Installing X-ray systems of point out contaminated mails costings millions
3. A study revealed that more people preferred driving rather than going by plane, even if that means more spending in terms of time, leaving out the cost of fuel, discomfort and even money.
4. Demonstrating a level of concern vastly disproportionate to the actual threat of infection.
Fed up by the constant monitoring of cameras which identify individual faces a group of Dutch researchers came up with a security technology which enabled privacy called the PrivaCam. This video surveillance output of these cams were broken down into data feeds and every individual would have access to only one feed at a time! Only if all data streams are put together the actual video would make any sense. Other technologies were also developed like IBM Privacy Research Institute developed cameras that blocked out faces with any trace of time or location associated with the feed.
Technology Proliferation time: Total Information Awareness

→ Hand scanners
→ Iris scanners
→ Thumbprint
→ Fingerprint
→ Handwriting scanners
→ ID cards and Smart cards
→ Brainwave scanners (To detect a lie)
→ Data mining and Data profiling technologies
→ Web identity scanners
→ Social media scanners

So there is nothing good or evil about these technologies which intended to separate out terrorists from law abiding citizens. The fact always circled back on how effective was this technology to combat threats could never be calculated.
Since the public does not demand technologies which will protect both privacy and security at the same time, the manufactures of these technologies are not inclined to build them on their own.

A study shows us that all technologies adapted by the government can be redesigned in a way so as to strike a balance between privacy and security at the same time.
“War is the health of the state... It automatically sets in motion throughout society those irresistible forces for uniformity, for passionate cooperation with the Government in coercing into obedience the minority groups and individuals which lack the larger herd sense.”

- Solidifies public opinion
- Close into the herd for protection, conform
- Demand for personal security
- Require judicial oversight for proposals and legal excesses
Libertarians of both the Left and Right came together in the debates over the Patriot Act
  ▶ Total Information Awareness
Separation of powers led to interesting observations about Congress and the courts
  ▶ Courts were more reluctant to challenge popular conceptions of privacy
  ▶ Congress, libertarians and religious conservatives mainly, sought to protect liberty and privacy
In the wake of the act passing, the executive branch was resisting providing information to the judiciary committee
Due to the efforts of Patrick Leahy and Russell Feingold, as well, half of the new surveillance policies in the Patriot Act would expire in 4 years
Technological Incompetence

- Moderates in Congress were halted by their lack of knowledge of the tech
  - Were not interested in regulating databases and profiling systems
- All barriers on information sharing between departments and agencies were broken down
- Suggested limiting use of information sharing and broader surveillance to only prosecute the most serious of crimes.
  - Poor precedent for these limitations lasting
- Congress more suited to ensuring surveillance tech remains within the law
- Courts generally cater to public opinion at the cost of privacy
  - Now due to importance of Supreme Court bids during presidential elections
  - Unclear constitutional grounds, few restrictions on surveillance
Desire for control over exposure

- What is wanted is not control over privacy, but control over exposure
  - Fine to violate privacy at the expense of others
  - Wish to be under illusion of control of personal information
  - Due to presence of potential stigma or prejudice
Chapter 5: Wish for connection

- The Naked Crowd wants a sense of emotional connection with everyone it encounters
- Pressure to reveal personal information
  - Due to:
    - Attempting to uphold some sort of identity
    - Guide who to trust
    - Prove value and trustworthiness
- Born as a result of horizontal society
  - As well as to establish one’s “brand”
  - To simplify one’s identity, make it predictable
Connect

- Create a personal “brand” to emotionally connect
  - Unreliant on morality
- Urge to simplify the complexities of the individual
  - Make it easy to remember (adjectives, descriptions)
- Public opinion allowed to greatly affect the individual
  - Individuality becomes impossible
- Poor attempt at exercising control over self-exposure
  - Illusion of control over privacy
  - Internet makes observation of individuals that much easier
  - Would rather be exposed than private