Nothing to Hide
The False Tradeoff between Privacy and Security

Jonathan Scrivanich & Trevor Miranda
About Us

- Jonathan Scrivanich
  5/5 Cybersecurity Undergraduate

- Trevor Miranda
  5/5 Cybersecurity Undergraduate
About the Author: Daniel J. Solove

- Professor of Law at George Washington University Law School
- Founder of “TeachPrivacy”
  - Company that provides privacy and data security training to institutions.
- Textbook author
- Internationally-recognized expert in privacy law
- Has testified before Congress
- Contributed amicus briefs to the Supreme Court of the US
Things to Come

Speaking Order:

1. First half - introducing concepts and issues
   a. Jonathan

2. Second half - viewing issues through the US Constitution
   a. Trevor
Introduction
I’ve Got Nothing To Hide

● Everyone has something to conceal.
  ○ “There is no sentient human being in the Western world who has little or no regard for his or her personal privacy; those who would attempt such claims cannot withstand even a few minutes’ questioning about intimate aspects of their lives without capitulating to the intrusiveness of certain subject matters.”

● George Orwell Metaphor-Big Brother

● Franz Kafka Metaphor-Information Processing
Problem with I’ve Got Nothing To Hide Argument

- Surveillance can inhibit such lawful activities as free speech, free association, and other 1st Amendment rights.
- Information Processing leads to suffocating powerlessness and vulnerability created by use of your personal data
  - Error, Frustration, lack of transparency, lack of accountability
- What is the extent which government can have this power of its citizens?
- Secondary use of collected data
  - While at the time may be harmless, may prove harmful in the future
- Distortion of collected data
  - Portrayed falsely and now have to worry about setting off red flags
Silencing Nothing-to-Hide

- The nothing-to-hide argument represents a singular and narrow way of conceiving privacy, and it wins by excluding consideration of the other problems often raised with government security measures.

- “the nothing-to-hide argument can ensnare, for it forces the debate to focus on its narrow understanding of privacy. But when confronted with the plurality of privacy problems the nothing-to-hide argument, in the end, has nothing to say.”
All Or Nothing Fallacy

- Sacrificing privacy doesn’t automatically make us more secure
  - Subway Monitoring System
- Security measures are often weighed against privacy rights yet this is wrong.
  - Fourth Amendment allows for wiretapping but limits the practice by mandating judicial supervision, minimizing the breadth and requiring a report back to prevent abuse.
- The choice is not between a security measure and nothing, but between a security measure with oversight and regulation and a security measure at the sole discretion of executive officials.
Privacy and Society

- Part of what makes a society a good place to live is the extent to which it allows people freedom from intrusiveness of others.
  - Avoiding oppression
- Individual rights are protections by society from its intrusiveness making space because of the social benefits this space provides
- Privacy constitutes society's attempt to promote civility
Pendulum Argument

- During times of crisis, the pendulum swings toward security and rights are curtailed.
- During times of peace, the pendulum swings back toward liberty and rights are restored.
- Argument: In times of crisis is when we should work our hardest in protecting privacy and liberty.
Pendulum Argument-Our History

- Unnecessary Sacrifices
- Often involve rights and liberties of minorities and dissidents. When people say they’re willing to give up rights and liberties in the name of security, they are often sacrificing the rights and liberties of others.
  - Civil War-President Lincoln suspended Habeas Corpus
  - WW1-Those who spoke out against the war were prosecuted
  - WW2-rounded up 120,000 people of Japanese descent and sent them to internment camps.
  - Cold War-Hundreds were subjected to interrogation and blacklisting for their communist belief
Pendulum Argument-Unhinged

- Hoping the pendulum will swing back offers little consolation.
  - Apologies are meaningless if one continues to make the same mistake
- Sometimes sacrifices in rights and civil liberties should be made
  - When government justifies the necessity
  - Subject these sacrifices to scrutiny
- “The greatest need for safeguarding liberty comes during times when we least want to protect it, when our fear clouds our judgment. We most need rights when the going gets tough—to stop us and make us think before we let our leaders hang Billy Budd.”
National Security-The Abuse

- Pentagon Papers revealing the government made deceptive claims about the Vietnam war
- "State Secrets Privilege" used to exclude evidence in a case that reveals a classified secret
  - Khaled El-Masri kidnapped by CIA and tortured. Was innocent. Tried suing.
  - Accident report of fatal air force plane crash.
- 1975 Church Committee of Congress
  - Revealed government surveillance activities focused on political agendas
  - Inspired creation of FISA
- As citizens of a democratic government we have a right to transparency and accountability of our governing officials
Criminal Investigation

- Electronic Communications Privacy Act (ECPA)
  - Strong protections of privacy
  - Requires officials to justify their belief that surveillance will uncover evidence of a crime
  - Explain to the court why alternative investigation is ineffective
  - Court's mandate minimizing listening when innocent people are involved
  - Strict scrutiny
Espionage (Spying)

- Foreign Intelligence Surveillance Act (FISA) established because the rule governing espionage are inadequate for protecting rights
  - Establishes procedures for officials to gather foreign intelligence within U.S. borders
  - Permissive affording much more expansive surveillance
  - Permits surveillance and covert searches after request is reviewed by a special “Foreign Intelligence Surveillance Court” which meets in secret
  - Longer surveillance
  - Surveilling can be kept secret indefinitely (unlike ECPA)
  - Doesn’t allow defendants to examine collect surveillance documents
Fall of Espionage Wall

- Patriot Act expanded FISAs scope from regulating espionage only when “the purpose” of was to gather foreign intelligence to the purpose of gathering foreign intelligence being “a significant purpose”
  - You can now be totally innocent to be surveilled since the goal is general information gathering
- Nazi Germany Gestapo blended these functions and Truman specifically said this would not be the same when creating the CIA
- “Espionage is a necessary function of government, but it is a dangerous and shadowy one, and it must remain confined lest it start polluting our constitutional democracy, where the government must be subjected to oversight and public accountability”
NSA Warrantless Search—"War Powers Argument"

- Claimed President’s constitutional powers include authority to conduct warrantless surveillance aimed at detecting and preventing armed attacks.
- Infirmity of the law
- Violated FISA
- Demands for security in the name of National Security should be subjected to the utmost scrutiny
US Constitutional Perspective
Fourth Amendment to the US Constitution

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
Fourth Amendment to the US Constitution

- Entire system of law enforcement regulated by this.
- Searches require **probable cause** to execute.
- You are protected by it when there is a **reasonable expectation of privacy**
Probable Cause?

Reasonably trustworthy information that a government’s search will turn up evidence of a crime.
Reasonable Expectation of Privacy

An individual’s perception of an interaction’s privacy (e.g. talking to someone in their home) and the objective expectation of privacy of a situation (e.g. walking around in a park).

(Note the complete lack of empiricism.)
Failure of Modern Interpretation

“The Fourth Amendment protects people, not places.”

*Katz v. United States decision excerpt*
Secrecy Paradigm

- Values physical intrusion over individual’s privacy when interpreting the Fourth Amendment.
- Has allowed modern government surveillance operations.
- Focus on privacy?
  - These breaches of privacy would be fewer and further between.
Third Party Doctrine

- If information is in the hands of a third party, **you have no reasonable expectation of privacy**.
  - Think: bank records, phone records, your search history
- If your files are in the cloud, they’re not considered private.
Your Digital Dossier

- Companies cannot meaningfully promise confidentiality
  - Governments do not have to oblige

- Government can promise confidentiality with consequences:
  - Census is confidential, disclosure of information is $250,000 fine and up to 5 years of jail time.

- Double standard?
Assumption of Risk Doctrine

● Telling another person a “secret” assumes a risk of betrayal.
● “If you assume the risk that your friends will betray you, then you likewise assume the risk that third parties holding your information will betray you.”
● Want privacy in the digital age?
  ○ Live in the woods.
Suspicionless Searches

“While the threat of terrorism is omnipresent, we cannot use it as the basis for restricting the scope of the Fourth [Amendment] ... there is no basis for using September 11 as an excuse for searching of ... [any] protesters.”

11th Circuit Court of Appeals in School of the Americas Watch vs. United States
“The US Supreme Court has increasingly recognized situations involving ‘special governmental needs, beyond the normal need for law enforcement’ where it is ‘impractical to require a warrant ... in the particular context.’

Daniel Solove
Exclusionary Rule

Bars evidence at a trial when the government gathers it in violation of the Fourth Amendment.

Provides: Fairness, Deterrence, and an Incentive to Litigate

Possible downsides?

● Could let criminals walk free!
  ○ Huge incentive for judges to reduce Fourth protections
Applying the First Amendment

- Chilling effect
  - Without caps on government surveillance, conversations that would have happened may no longer happen.
  - Subpoena journalists for sources, journalism is stifled.
  - (This could be construed as a First Amendment argument.)

- **First Amendment should be part of the discussion and used in criminal cases!**
Adjusting to New Technologies
Repeal the Patriot Act to Save Privacy?

- **What is it?**
  - It’s what made “metadata” collection entirely legal.
  - Content vs Envelope officially codified in law.
- **IP address collection (envelope)**
  - Harmless?
  - If I can see US Internet traffic, I can follow you!
- **National Security Letters existed before the Patriot Act**
  - **Conclusion:** The Patriot Act is not what killed privacy, but it helped.
Leave it to the Legislature!

- Legislation works faster than courts?
  - Show me the driverless car regulations!
- Statutes have to be broad to fit many circumstances.
  - Court cases tackle specific scenarios!
- 30 years passed between Electronic Communications Privacy Act and the Patriot Act!!!
There’s No Privacy in Public
Take your CCTV Surveillance To-go!

● No expectation of privacy in publicly-visible spaces.
  ○ Fourth Amendment **cannot** protect you from video surveillance at a massive scale.

● **Foreign Intelligence Surveillance Act**
  ○ Requires detailed court-order to surveil foreign spies.
  ○ Foreign spies have more rights against this kind of surveillance than US Citizens. (You can laugh here.)
Should the Government Mine Data?

- Patterns emerge from large data sets. Patterns can predict criminal behavior.
- If unconscious machines are doing it, no privacy violation!
- Problems?
  - If Amazon can’t predict you perfectly, the Government definitely can’t.
  - Where’s my due process? I can’t question an unconscious machine!
The Titanic Phenomenon

- Everyone rushes to new technologies without considering their consequences
- For example, biometrics
  - Huge privacy concerns (think *Minority Report*)
  - Yet, plenty of people are fine putting their children’s fingerprints into national databases in case of abduction.
    - Highly unlikely event, information ownership lost forever.
Ludditism

- Anyone who opposes new technology is a luddite!
  - The *Titanic* is unsinkable!!!

- “357 million records were compromised between 2005 and 2010.” (Solove)

Oops.
Fix-a-Problem Strategy

- “We have X problem, waiting to implement it has Y harms.”
  - “Sure, but why is X a problem?”

- Biometrics again
  - Why is identification so important?
  - Convincing cases should be made for claims before widespread adoption.
  - Don’t ignore problems, but don’t fall for hype.
Conclusion?

- Oversight, oversight, oversight!
  - (With fines and jail time as consequences!)
- Legislators should be cautious and specific with new technology.
- Mandating changes before adequate review is a bad idea!
- Privacy is more than just content-envelope.
- Privacy is more than just illegal searches! (First Amendment)
Thank you for listening!