

# Security/Privacy Ethics and Policy

COM-402: Information Security and Privacy

# Outline

- **Information Security Policy and Incentives**
- Security and Cryptography Standards
- The Crypto Wars: Privacy versus the State, Parts I and II
- Ethical Hacking and Responsible Disclosure Practices
- Data Protection Laws: US and Europe
- Privacy, Speech, Anonymity, and Accountability

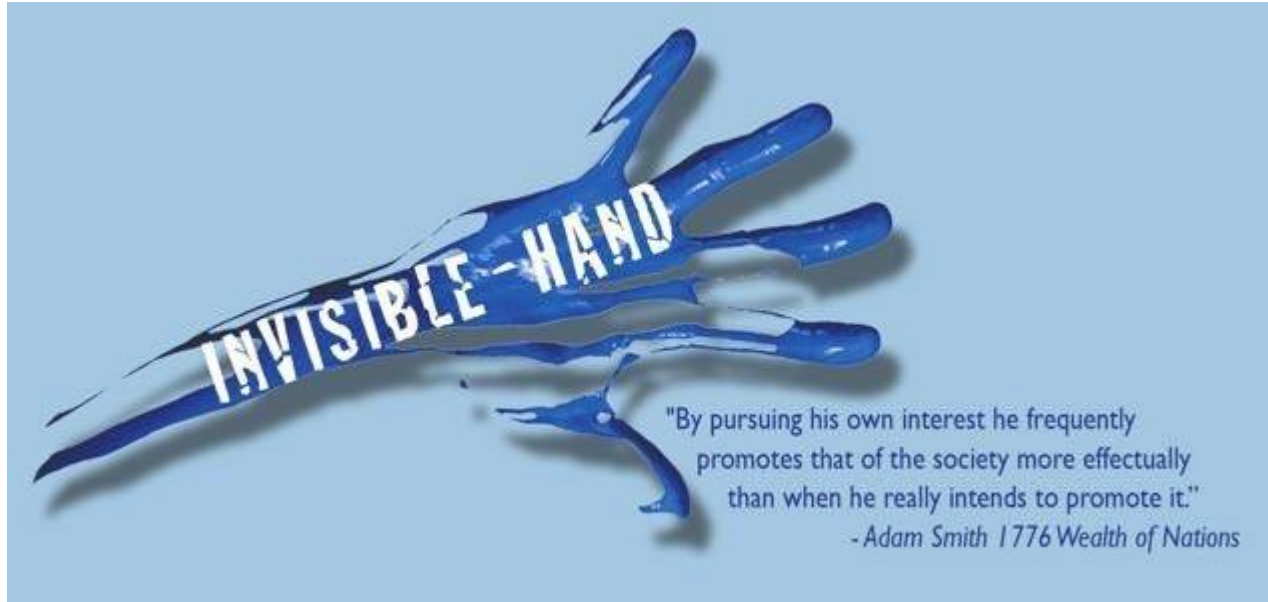
# Security/Privacy Policy and Incentives

Some key questions:

- Why does [Internet/Cyber] security suck?
- What incentives do (and don't) exist to maintain/improve security, privacy?
- What standards should apply to security and privacy of information?
- What responsibility/liability should companies processing PII have?
- What responsibility/liability should hardware/software vendors have?

# Market-Driven Security/Privacy

Why doesn't market competition "just work" and make things secure?  
We have Adam Smith's "invisible hand", right?



# Market-Driven Security/Privacy

Why doesn't market competition “just work” and make things secure?

Unfortunately:

- For most companies, security is a product cost, not a salable feature
  - More security means longer development, higher costs, risk of losing race to market
- Hard for customers to distinguish strong security from empty claims
- Many companies have incentives *not* to compete on security
- Security companies incentivized to sell easy-to-deploy add-on “solutions”
- Silicon Valley business model: “free” services funded by selling user data

# The Market for Lemons

Nobel Prize-winning economist  
George A. Akerlof observed:

When buyers have much less information  
than sellers about the quality of products,  
incentives drive sellers to reduce quality

- Seller knows low-quality lemons are faster and cheaper to produce
- Buyer can't [immediately] distinguish



# The Market for **Security** Lemons

Unfortunately:

- Sellers of information systems know their investment in security
- Buyers can't readily discern



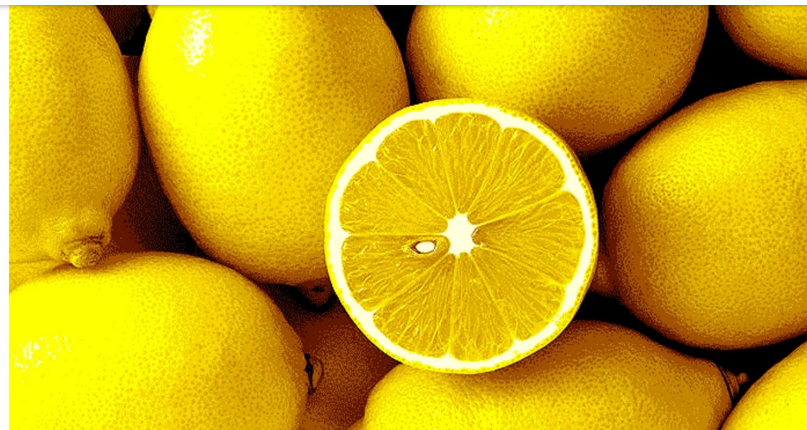
## Schneier on Security

[Blog](#) [Newsletter](#) [Books](#) [Essays](#) [News](#) [Talks](#) [Academic](#) [About Me](#)

[Blog](#) >

### A Security Market for **Lemons**

More than a year ago, I [wrote](#) about the increasing risks of data loss because more and more data fits in smaller and smaller packages. Today I use a 4-GB USB memory stick for backup while I am traveling. I like the convenience, but if I lose the tiny thing I risk all my data.



## Cyber Security and The Market for Lemons

Published on February 18, 2015 | Featured in: [Information Privacy & Security](#)



Joe Cocchini [Follow](#)



29



2



0

IT SEEMS THAT THERE IS A MARKET FOR SOFTWARE LEMONS.

# Companies Avoid Competing on Security

Companies in security-critical businesses, e.g., banks, agree not to compete with each other on the basis of security. Why?

*“I learned long ago, never to wrestle with a pig. You get dirty, and besides, the pig likes it.” - George Bernard Shaw*

Result is that potential customers become suspicious and mistrustful of *all* companies' security (e.g., of online banking in general)



[photo credit: [Gregory Kuhn](#)]



# Selling Security in a Box

Companies that *do* focus on security prefer easy-to-sell “drop-in” solutions

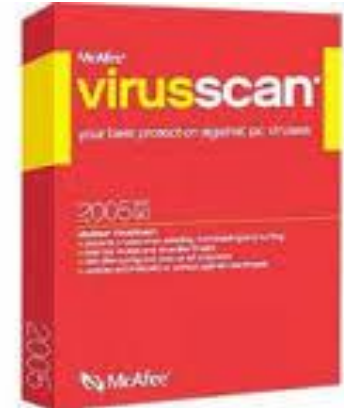
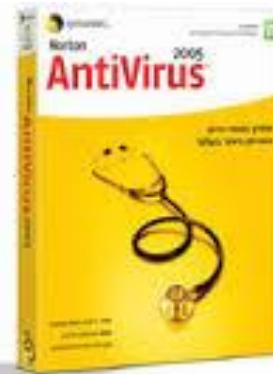
- Devices for customers to attach to existing networks



# Selling Security in a Box

Companies that *do* focus on security prefer easy-to-sell “drop-in” solutions

- Devices for customers to attach to existing networks
- Software to install on existing machines



# The Problem

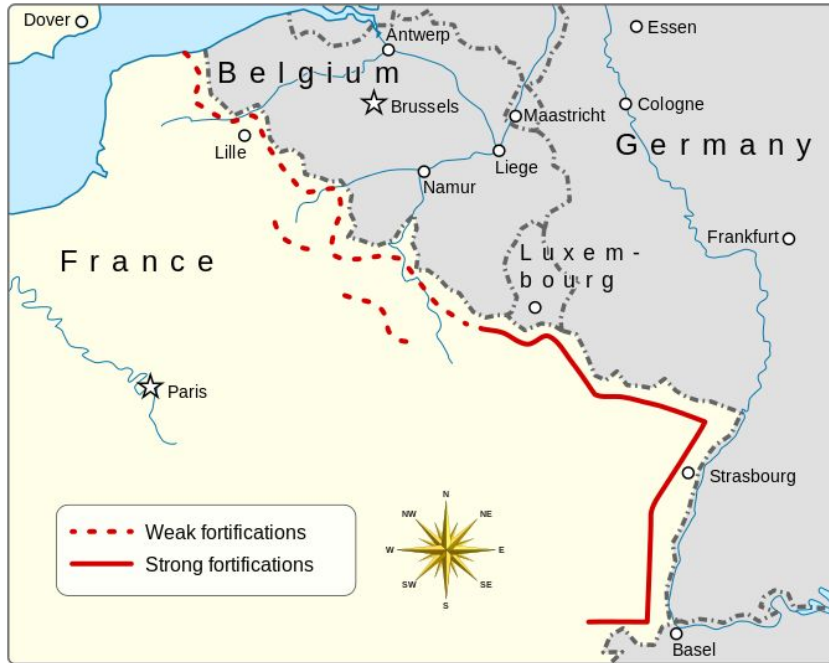
The fundamental problem is that security is a cross-cutting concern

- Information systems tend to be insecure unless *pervasively* built for security throughout the architecture, design, and implementation process

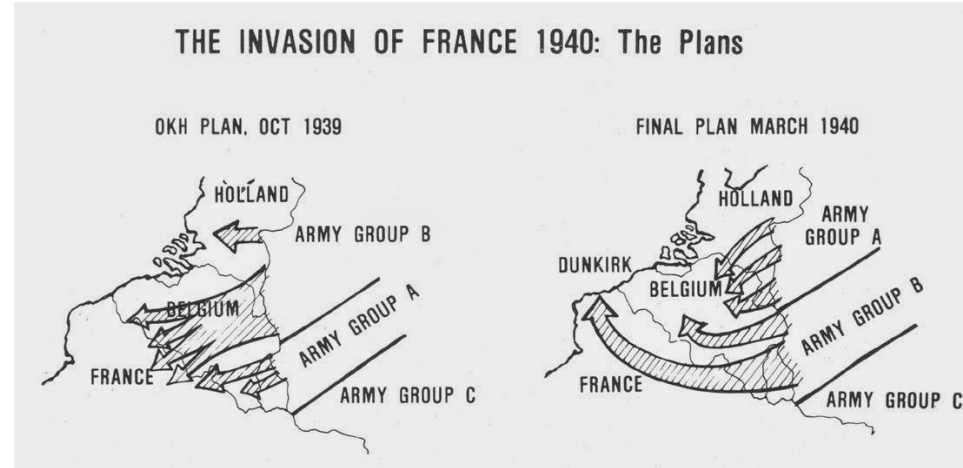
Pursuing security through add-ons is like France's defense against Germany in WWII...



# WWII: The Maginot Line



[credit: [Wikipedia](#)]



[credit: [Andrew Lynch](#)]

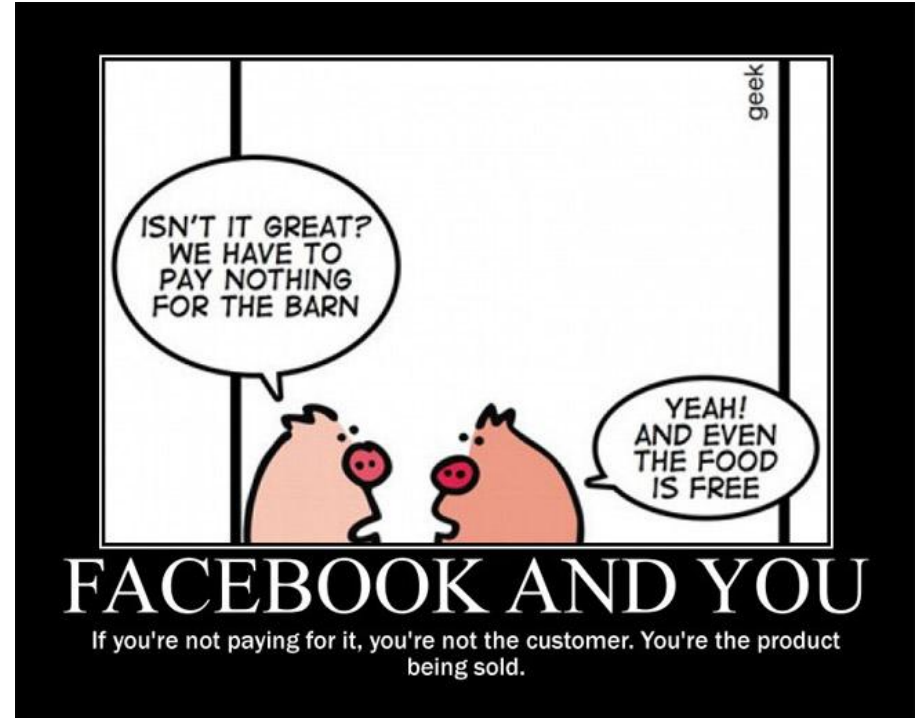
# The Silicon Valley Business Model

People seem to like “free” stuff

- Internet searches, social networking, games, news...
- If it's available for free, why pay for a non-free/paywalled alternative?

Free services funded by selling data

- User tracking, profiling
- Targeted advertising

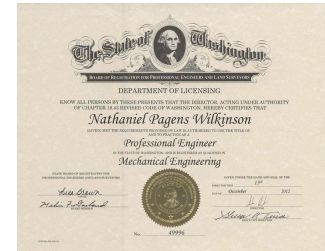


# Security Policy and Incentives

It's increasingly commonly-recognized that “the free market” alone isn't sufficient to drive improvements in information security - but then what?

Some policy approaches:

- Standardized algorithms, processes for security
- Independent evaluation authorities
  - Vendors submit product for security testing to get “seal of approval”?
- Professional licensing
  - Should “security engineers” be like doctors, lawyers, accountants, ...?
- Legal liability for security/privacy failures



# SpeakUp

<https://web.speakup.info> - Room 71839

How do you handle security on your computer?

- A. Always update all the programs to the latest version
- B. Using obscure OS ([Qubes OS](#))
- C. Additional Firewall + Antivirus (not the one from the OS)
- D. Being careful what I click on the internet
- E. Nothing of this list

# Outline

- Information Security Policy and Incentives
- **Security and Cryptography Standards**
- The Crypto Wars: Privacy versus the State, Parts I and II
- Ethical Hacking and Responsible Disclosure Practices
- Data Protection Laws: US and Europe
- Privacy, Speech, Anonymity, and Accountability



# Security Standards

US NIST produced widely-used FIPS standards including cryptographic algorithms such as DES, AES, SHA-\*

Can be adopted **voluntarily** or **involuntarily**



- Voluntary uses (e.g., commercial):
  - Advantage: reduces prevalence of bad, often completely broken, ad-hoc alternatives
  - Disadvantage: only partial solution; easy and common to misuse standards insecurely
- Mandatory uses (e.g., FIPS-compliance requirements in defense contracts):
  - Advantage: in principle, you know that it's been done in "the approved way"
  - Disadvantages: implementation bugs remain; can chill innovation; do you trust the standards?

# Standards Gone Wrong: DUAL\_EC\_DRBG

NIST-standardized FIPS  
algorithm for cryptographic  
random number generation

- Cryptographers observed in 2005 it *might* have backdoor
- Confirmed in 2013 as part of Snowden leaks

Many people now trust [US]  
crypto standards a lot less...



# Outline

- Information Security Policy and Incentives
- Security and Cryptography Standards
- **The Crypto Wars: Privacy versus the State, Parts I and II**
- Ethical Hacking and Responsible Disclosure Practices
- Data Protection Laws: US and Europe
- Privacy, Speech, Anonymity, and Accountability

# Governments and Encryption

Key recurring issue: how to “balance” the rights of individuals to information privacy against the needs of governments to pursue criminals, terrorists, etc?

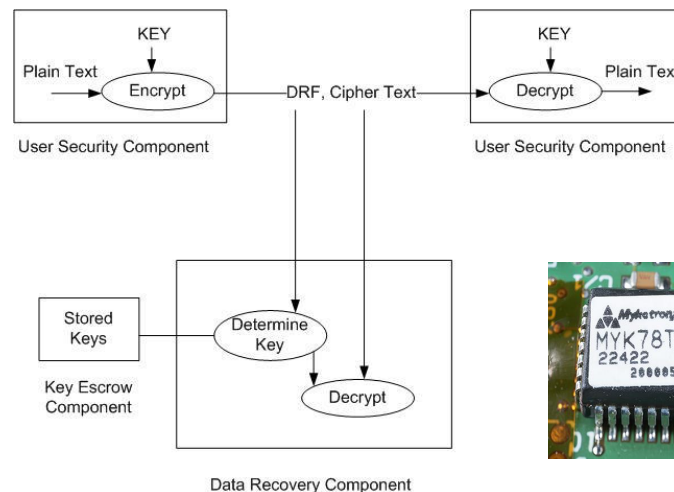
- How strong is the right of individuals to keep personal data private?
- Are governments entitled to be able to decrypt encrypted personal data?
  - If so, at what legal threshold: Reasonable suspicion? Probable cause?
  - How broad or targeted must governmental collection of user data be?
  - How to avoid convicting someone although he's innocent?

# Crypto Wars Part I: The Clipper Chip

In the 1990s, US government wanted to introduce an encryption standard called **Skipjack**, embodied in the **Clipper chip** (hardware implementation), which included a **key escrow** function.

- Keys normally private to two users (Alice, Bob)
- But a key recovery mechanism allows government access if needed

Heavy popular backlash, ultimately failed



# Crypto Wars Part II: The Continuing Saga

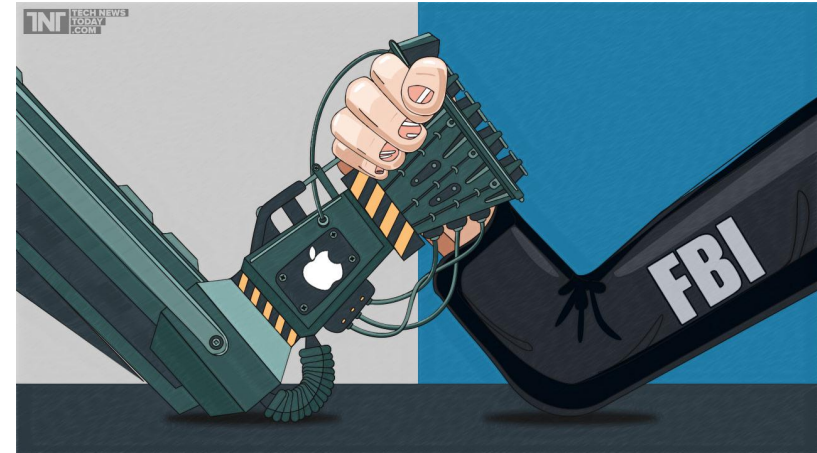
Prompted in part by Snowden leaks,  
tech companies trying to strengthen privacy,  
e.g., with end-to-end encrypted chat



# Crypto Wars Part II: The Continuing Saga

Prompted in part by Snowden leaks, tech companies trying to strengthen privacy, e.g., with end-to-end encrypted chat

Law enforcement agencies such as FBI, having difficulty decrypt criminals' or terrorists' data, pressuring tech companies to create back-doors or “golden keys”...



# The Crypto Wars

A few key issues - for more, read [schneier.com](https://schneier.com):

- Back-doors are security weaknesses introduced intentionally
- Such weaknesses tend to get misused, exploited in unexpected ways
  - Master keys get leaked or stolen, used by criminals or foreign powers
  - Hackers figure out how to exploit bugs in complex, rarely-tested backdoor code
- Law enforcement positions based on search warrant, telephone wiretap law
  - US constitution allows government to search home, possessions based on Probable Cause
  - Established when tapping could be done at central “switchboards”
- But US Constitution and legal practice also protects against self-incrimination
  - Even if I know I’m a criminal and remember the crime, I have the right to “plead the 5th”
- Are personal devices more like homes or like extensions to our minds?



# SpeakUp

<https://web.speakup.info> - Room 71839

The government should have access to my data/communication:

- A. At all times - I don't have anything to hide
- B. Only when a judge allows it
- C. Never
- D. Only for terrorists - they should be targeted

# Outline

- Information Security Policy and Incentives
- Security and Cryptography Standards
- The Crypto Wars: Privacy versus the State, Parts I and II
- **Ethical Hacking and Vulnerability Disclosure Practices**
- Data Protection Laws: US and Europe
- Privacy, Speech, Anonymity, and Accountability

# Hacking around

- Software system inherently have bugs
- **Legal and monetary incentives** for finding and disclosing security bugs
- Choose your destiny: black hat, gray hat or white hat

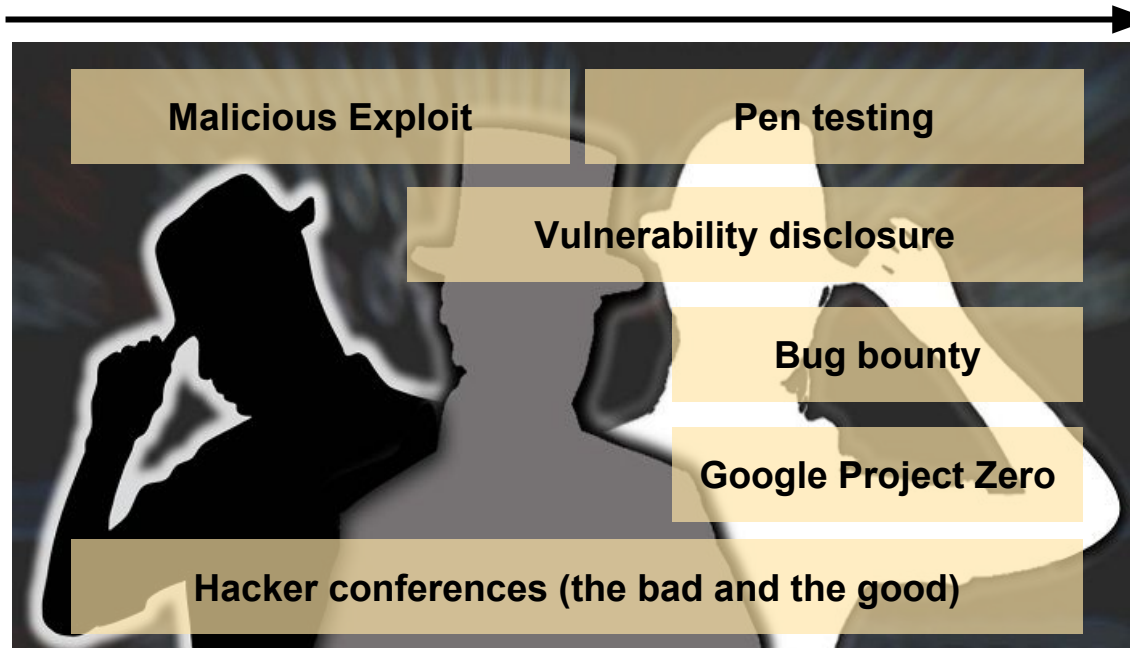


<http://hackingig.com/what-are-the-types-of-hackers/>

# Roadmap

**Unethical  
Hacking**

**Ethical  
Hacking**



# Penetration Testing

- Hacker hired by company to perform security analysis of its systems / employees
- Only few people of the company, who authorized the hacking, are aware of it
- Finds software, network and people vulnerabilities
  - Port scanning
  - Stress tests
  - Status of system patches
  - Web applications
  - Social engineering of employees (passwords, policy with USB sticks)
- Network pen test practices, e.g., [Cisco's art-of-hacking series](#)
- Certifications available, e.g., [Offensive Security Certified Professional \(OSCP\)](#)

# Vulnerability Disclosure

- Practice of reporting discovered security flaws in a system

Disclosure Models	
<b>Full Disclosure</b>	<ul style="list-style-type: none"><li>● Vulnerability is published as soon as it is discovered.</li><li>● If customers are aware, vendors are pressured to fix the issue!</li><li>● Not very responsible: attackers can exploit the unpatched vulnerabilities and put customers at risk.</li></ul>
<b>Coordinated Disclosure</b>	<ul style="list-style-type: none"><li>● Vendor is first made aware of the vulnerability.</li><li>● CERT (Computer Emergency Response Team) is informed.</li><li>● Public disclosure usually after 45 days.</li><li>● Gives the vendors time to develop and release patches.</li></ul>
<b>Non Disclosure</b>	<ul style="list-style-type: none"><li>● Vulnerability information is not shared or shared only under NDA (non disclosure agreement)</li></ul>

# Bug Bounty Programs

- Companies offer financial reward to individuals who discover vulnerabilities
- But other sources pay more. For a system exploit in iOS
  - Apple gives up to 200'000 US\$
  - Other companies pay 500'000 US\$ or 1 million for the same bug

Where would you submit?

- Sometimes companies don't pay up
- Other bugs might stay hidden in a military

# Example: Google Project Zero

- **Example of ethical hacking and ethical vulnerability disclosure practice**
- Team of security researchers at Google whose aim is to discover vulnerabilities in software products.
- Why “Zero”?
  - Aim is to find zero-day vulnerabilities
  - Zero-day vulnerabilities are those that have been unknown so far.
- Team reports vulnerability findings to the vendor first so that they can release a patch.
- Findings are made public when the patch is released or 90 days after the vendor was informed (responsible/coordinated disclosure).



# Hacker Conferences

- Events where security professionals, enthusiasts, agencies meet for training, talks, wargames and social events
- Famous conferences: DEF CON and Black Hat (together sometimes known as “Hacker Summer Camp”)
  - Black Hat is considered to be more targeted towards corporate security
  - DEF CON is considered more informal
- Vulnerabilities are often disclosed and described during these conferences
- Not all participants are well intentioned



# SpeakUp

<https://web.speakup.info> - Room 71839

What would you do if you discovered a 0-day root exploit on iOS?

- A. Keep it to myself and use it for creating my own hacker kit
- B. Sell it to the most offering on the darknet
- C. Get a bug-bounty from Apple
- D. Post it on twitter

[Comparing payouts](#)

# Outline

- Information Security Policy and Incentives
- Security and Cryptography Standards
- The Crypto Wars: Privacy versus the State, Parts I and II
- Ethical Hacking and Responsible Disclosure Practices
- **Data Protection Laws: US and Europe**
- Privacy, Speech, Anonymity, and Accountability

# Laws and Liability for Information Security

Can the law force companies to keep their stuff secure?

Sometimes, but:

- Relevant laws vary widely across countries, even across Europe
- Companies try to avoid liability, e.g., through “click-wrap” agreements

# Legal Liability

By default, companies like to **avoid liability**

Use “click-wrap” agreements to claim:

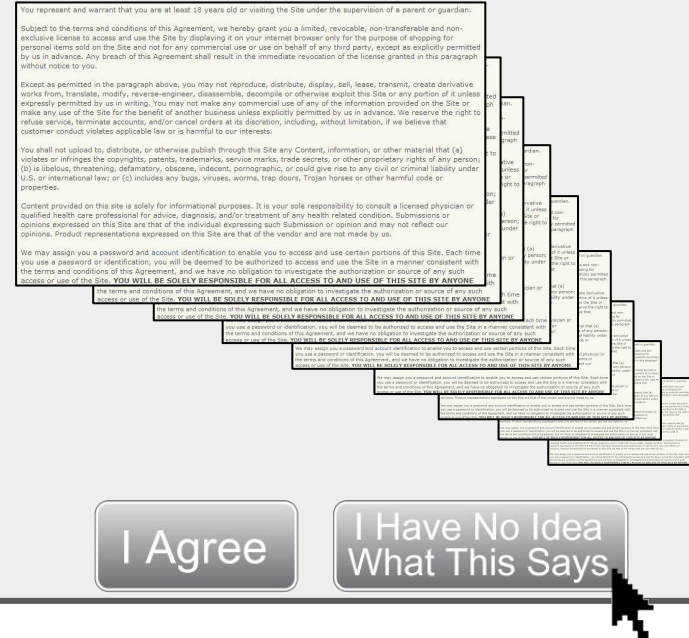
- We own all your data
- We can do anything we want with it
- You can't sue us for anything ever
- Disputes to be arbitrated on the Moon

Who reads these agreements?

What terms are “reasonable”?

What terms are legally enforceable?

By clicking OK you agree that:



The screenshot shows a typical 'click-wrap' agreement interface. It features a large, dense block of legal text in a small font, which is mostly illegible. At the bottom of the screen, there are two buttons: "I Agree" and "I Have No Idea What This Says". A mouse cursor is clicking on the "I Have No Idea What This Says" button. The text in the background is a standard legal disclaimer, including a warranty of age, a statement of agreement to the terms, and a statement of understanding that the user is responsible for their actions. The interface is designed to make the user feel that they are agreeing to something without fully understanding the terms.

# Data Protection Laws

Laws can establish standards for data protection that apply to all users

- Users can sue for violations regardless of what click-wrap agreements say

But data protection laws have been slow to adapt and widely varying

- Traditionally stronger in Europe than US
- But evolving, widely varying by country
- Hard for both users & companies to track

EU's GDPR standardizes data protection

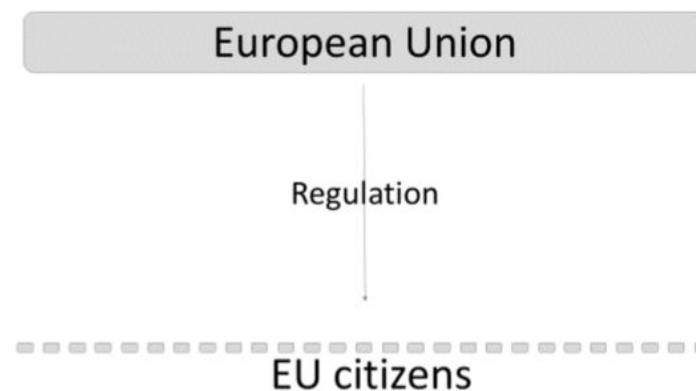
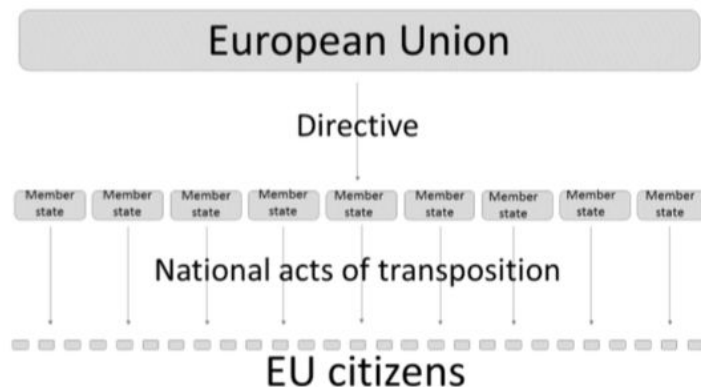


- Adopted by EU in April 2016, will take effect on 25th of May 2018

# EU Directives vs Regulations

- **EU Directives** – not directly applicable but implemented in each Member State through domestic legislation

- **EU Regulations** – directly applicable in the **same way** in each Member State



# Leading Actors in GDPR Land



[credit: [Ramiro Cid](#)]



# Key Provisions of the GDPR

- Data collection must be reported to data protection authorities
- Certain types of organizations required to appoint a DPO
- Users must explicitly give consent to collection and use of personal data
- Mandatory Privacy Impact Assessments (PIAs) before data collection
- Violations of data protection (e.g., breaches) must be reported within 72 hours
- Data minimization: keep data no longer than necessary, only for original use
- Right to be forgotten: users can demand data about them be deleted
- Extends liability beyond Data Controllers to Data Processors (outsourcing)
- Enforceable against *any* company based anywhere in the world
  - By fines up to 20M Euro or 4% of annual turnover

# Data Protection: The US Approach

Ad hoc, dependent on type or usage of data

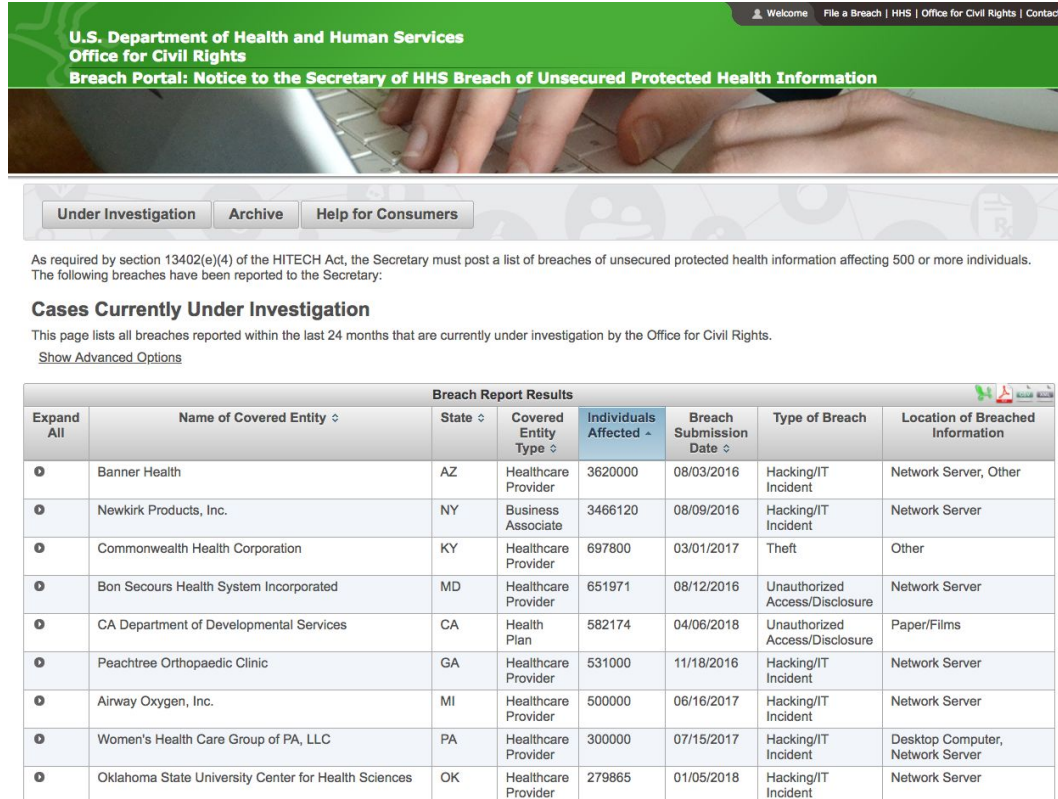
- Health Insurance Portability and Accountability Act (HIPAA): health data
- Fair Credit Reporting Act (FCRA): consumer credit data
- Electronic Communications Privacy Act (ECPA): networked communications
  - Broad but weak: many large loopholes, provisions easily circumventable



# Transparency: US HIPAA “Wall of Shame”

A “transparency carrot”  
approach to liability

- If vendor discovers and discloses breach, liability limited to fixed amount
- If vendor discovers and **fails** to disclose breach, liability is **unlimited**



Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Banner Health	AZ	Healthcare Provider	3620000	08/03/2016	Hacking/IT Incident	Network Server, Other
	Newkirk Products, Inc.	NY	Business Associate	3466120	08/09/2016	Hacking/IT Incident	Network Server
	Commonwealth Health Corporation	KY	Healthcare Provider	697800	03/01/2017	Theft	Other
	Bon Secours Health System Incorporated	MD	Healthcare Provider	651971	08/12/2016	Unauthorized Access/Disclosure	Network Server
	CA Department of Developmental Services	CA	Health Plan	582174	04/06/2018	Unauthorized Access/Disclosure	Paper/Films
	Peachtree Orthopaedic Clinic	GA	Healthcare Provider	531000	11/18/2016	Hacking/IT Incident	Network Server
	Airway Oxygen, Inc.	MI	Healthcare Provider	500000	06/16/2017	Hacking/IT Incident	Network Server
	Women's Health Care Group of PA, LLC	PA	Healthcare Provider	300000	07/15/2017	Hacking/IT Incident	Desktop Computer, Network Server
	Oklahoma State University Center for Health Sciences	OK	Healthcare Provider	279865	01/05/2018	Hacking/IT Incident	Network Server

# SpeakUp

<https://web.speakup.info> - Room 71839

GDPR and me:

- A. Never heard of it before
- B. I've been asked by friends who have an organization
- C. I had to revamp the organization I'm part of due to the GDPR
- D. I got elected as a DPO

# The 10 Commandments of GDPR

1. Document what personal data you hold
2. Appoint a representative (or Data Protection Officer)
3. Review your current privacy notices
4. Identify the lawful basis for the processing activities
5. Review how you seek consent
6. Prepare for individuals to exercise their (many) rights
7. Verify individuals ages
8. Set up a process in case of data breaches
9. Adopt Privacy by Design and by Default approach
10. Carry out Data Protection Impact Assessments

<https://francoischarlet.ch/2017/gdpr-in-switzerland-10-steps-to-take/>

# Outline

- Information Security Policy and Incentives
- Security and Cryptography Standards
- The Crypto Wars: Privacy versus the State, Parts I and II
- Ethical Hacking and Responsible Disclosure Practices
- Data Protection Laws: US and Europe
- **Privacy, Speech, Anonymity, and Accountability**

# Privacy and Online Speech

The Internet was seen as friendly toward privacy and anonymity since its inception...

- Text-only communication
- Easy to masquerade as anyone
  - Hide behind pseudonyms, IP addresses



*"On the Internet, nobody knows you're a dog."*

[credit: [The New Yorker](#)]

# Privacy and Online Speech

The Internet was seen as friendly toward privacy and anonymity since its inception...

- Text-only communication
- Easy to masquerade as anyone
  - Hide behind pseudonyms, IP addresses

Seen as empowering marginalized groups

- Safe online forums to meet, discuss with like-minded people
- Avoid real-world intimidation, threats

## Queers Anonymous: Lesbians, Gay Men, Free Speech, and Cyberspace

---

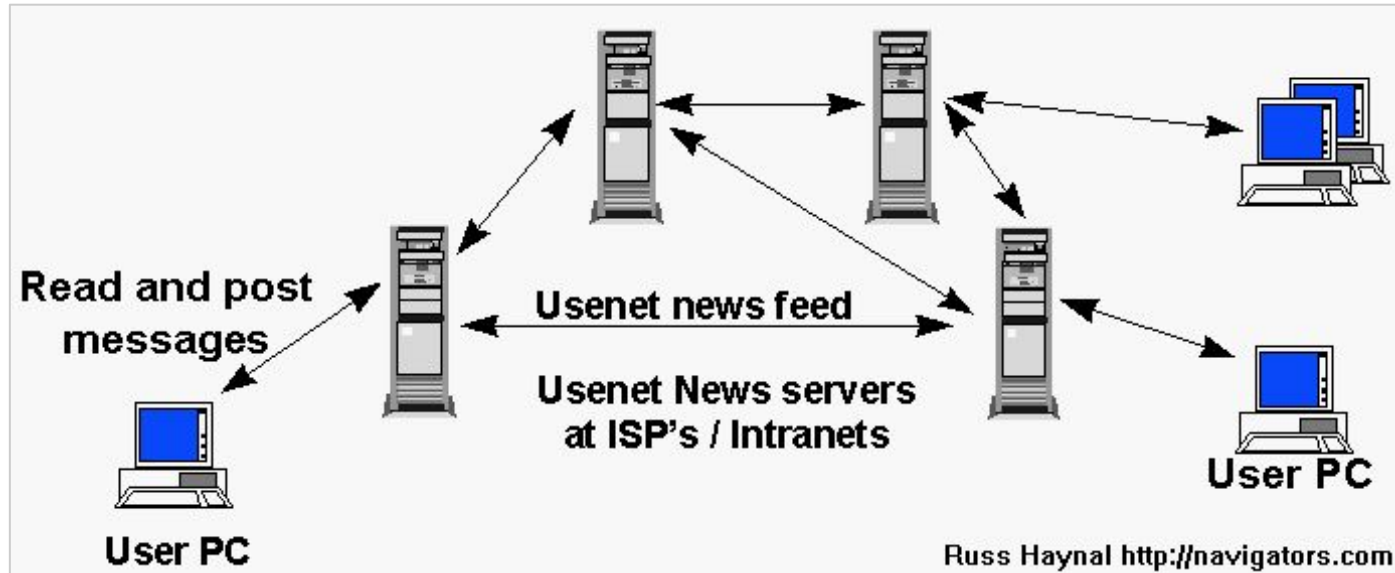
*Edward Stein\**

Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society.<sup>1</sup>

Pseudonymity allows people who are experimenting with different sorts of interests to do so without social repercussions. People can temporarily obscure their real life and play with a different conception of what their life might be.<sup>2</sup>



# USENET: The Original Online Forum



[credit: [Russ Haynal](http://navigators.com)]

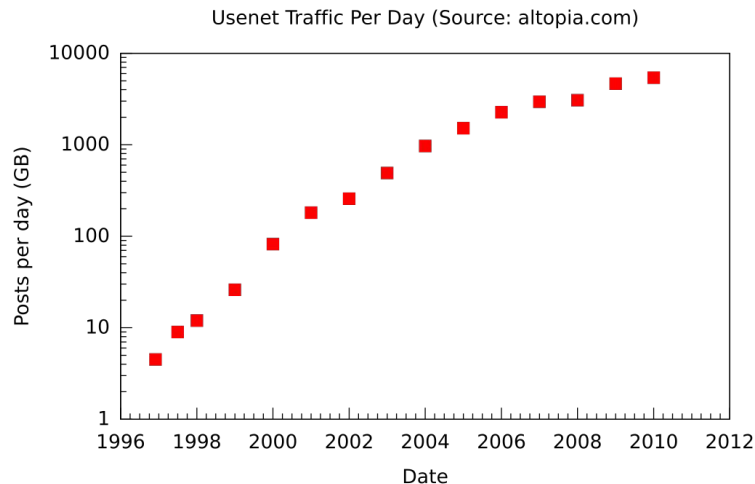
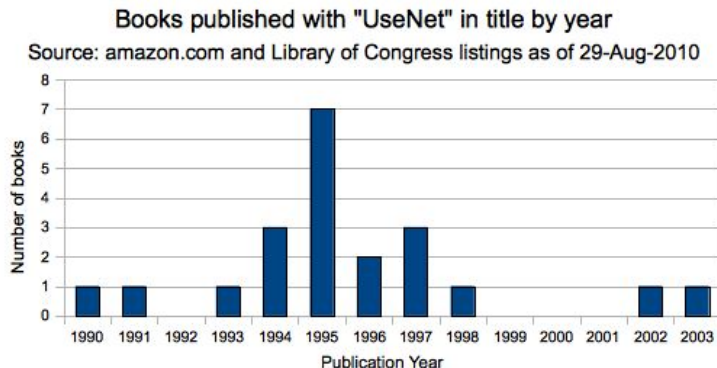
# The “Death” of USENET



USENET had no effective spam control

- No user authentication or accountability
- Group moderation circumventable

Spammers arrived, users fled to private forums

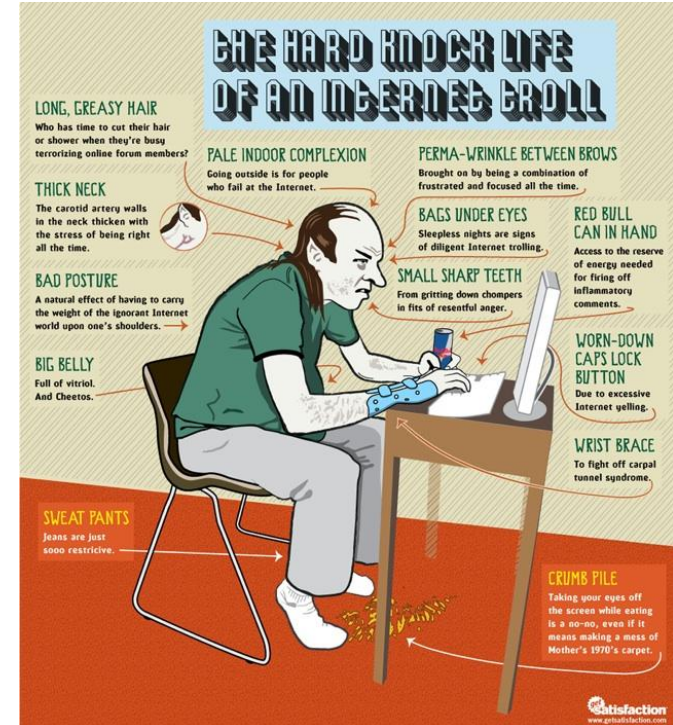


[credit: [Wikipedia](#)]

# Internet Trolling

Now a ubiquitous problem

- Persistent verbal abuse against a target
- Sometimes threats of physical violence
- Doxing: broadcasting sensitive personal data (e.g., home address, cell phone number)
- Revenge porn: publishing sensitive personal images, videos, stories, ...



[credit: [Ariana Lao](#)]

# Internet Trolling

Exacerbated by **Sybil attacks** or **Sock-Puppetry**:  
one troll controls many personas

- Ban one, troll just creates more

Persistent problem in deliberative forums

- e.g., Wikipedia discussions:  
troll's position supported by sockpuppets

As a result, even “anonymity-friendly” forums like  
Wikipedia often forbid anonymous login/editing



[credit: [SmallBusiness.com](https://www.smallbusiness.com)]

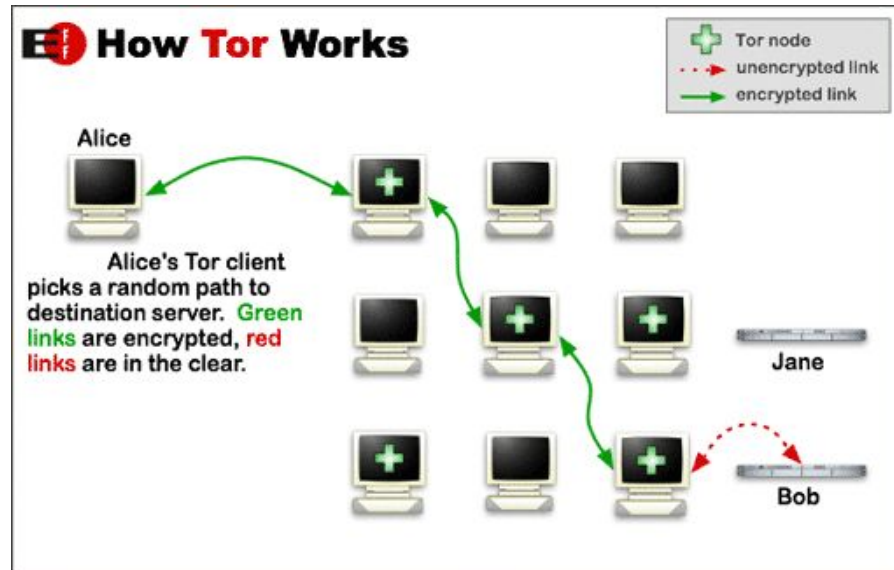
# Anonymity versus Accountability

Since IP addresses don't provide strong anonymity, privacy community created tools to provide stronger anonymity...

- Paid VPN services
- Tor: The Onion Router

Research producing many new “next-gen” anonymity systems

- Dissent, Herd, Riposte, Vuvuzela, Riffle, ...



# Anonymity versus Accountability

But even die-hard privacy advocates eventually get sick of trolls...

## That Time a Tor Developer Doxed a Troll

FE FRUZZINA EORDOGH  
Dec 3 2014, 1:00pm



**The events that led to the unmasking of Jeremy Becker.**

Doxxing, where someone's personal information is published online as an act of digital vigilantism, has become so common even privacy and anonymity advocates are doing it.

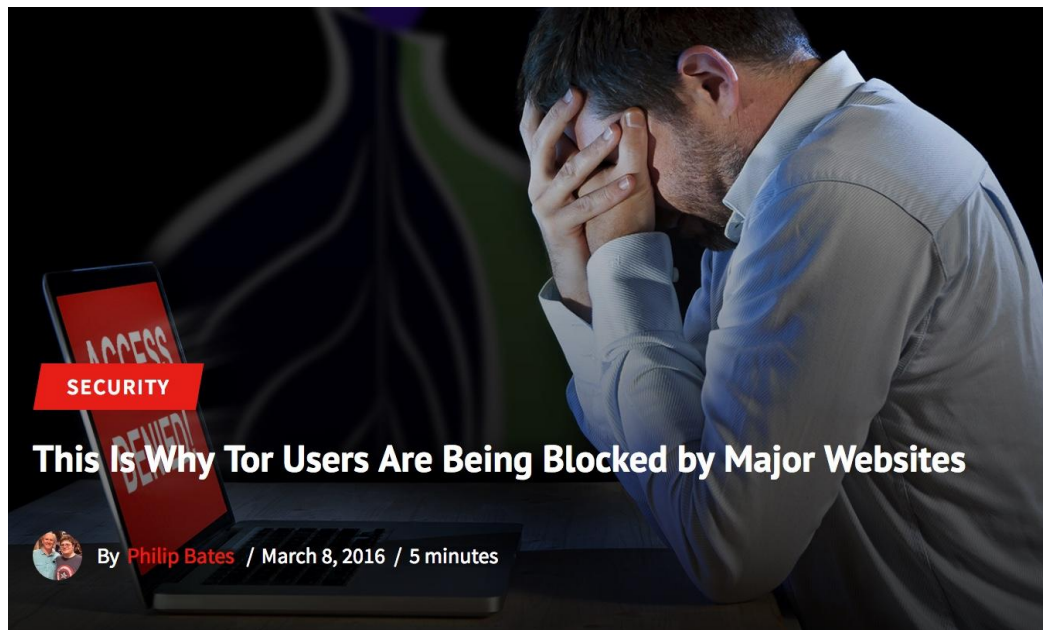
[credit: [Motherboard](#)]

# Anonymity versus Accountability

But even die-hard privacy advocates eventually get sick of trolls...

And many web sites are banning anonymous users

- There may be many well-behaved users...
- But a few trolls and all their sock-puppets can “spoil the barrel”



[credit: [MUD](#)]



# Fake News and State-Sponsored Trolling

Are nation-states getting  
into the trolling business?

Can trolling be so effective  
as to win elections?



[credit: [Brandon Martinez](#)]



# Fake News and State-Sponsored Trolling

Are nation-states getting into the trolling business?

Can trolling be so effective as to win elections?

- Using human-operated and bot-operated fake personas to push news
- Fear, uncertainty, doubt (FUD)
- Undermine “truth”



[credit: [Tom Dougherty](#)]

# Privacy vs Accountability: Fundamental conflict?

**Inherent conflict** that boils down to strengthening or weakening source IP addresses

- **Accountable Internet:** source IP addresses undeniably link packets to senders
- **Private Internet:** senders hide source addresses as much as possible



Research to fulfill both **changes Layer 3**

- Use two addresses: sender identity and return address
- [“Accountable and Private Internet Protocol”, Naylor et al., SIGCOMM’14](#)

# Privacy vs Accountability: PoP Parties

**Proof of Personhood (PoP):** Organize a party where people are verified (i.e., the person is real) by giving *one* cryptographic token to *one* attendee.

- Usage: each attendee can create a signature to prove to a service that he was part of the party
- The service however cannot link the signature to any of the public keys
- BUT: the service can link a signature to a pseudonym within a context
  - For voting: each attendee can only vote
  - For wikipedia: trolls can be excluded
- BUT: voting and wikipedia cannot collude to de-anonymize the signatures



# Blockchain Proof-of-Individuality

Same idea as PoP parties, but instead of in-person meetings, it relies on periodic video conferences.

- You cannot be in two places / two video calls at the same time without the participants noticing
- Participants sign each-other's POI (proof of individuality) token using **Ethereum smart contracts**
- Gas for this contract: anti-spam deposit
- POI's are indexed on Ethereum and searchable



# Privacy, Speech, Anonymity, Accountability

A few key questions:

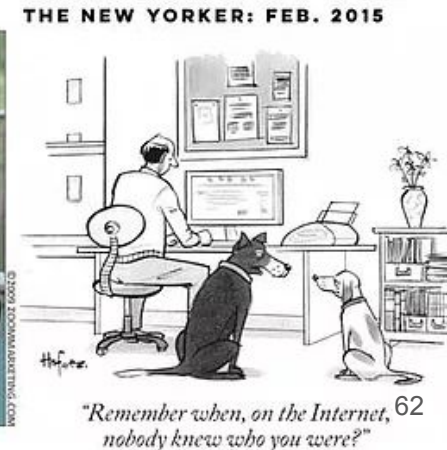
- What mechanisms are necessary and sufficient to deter trolling?
- How to protect (or reintroduce) “truth” in the online world?
- Is it possible to have forums with both unconditional freedom of speech while providing protection against spam and abuse?
  - Example: mechanisms to enforce “1-person-1-pseudonym” relationship

# SpeakUp

<https://web.speakup.info> - Room 71839

Things that *should be forbidden* regardless **Freedom of Speech**

- A. Religious discussion and criticism
- B. Incitement to criminal behaviour
- C. Libel / Slander
- D. Child abuse
- E. Criticism of government
- F. Terrorist propaganda



# Conclusion

- Security is hard and needs to be incentivized from the outside
- Privacy versus the State
  - "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." - Benjamin Franklin
- Ethical Hacking and Responsible Disclosure Practices
- GDPR is coming - let's hope it helps us (except in Switzerland)
- Anonymity vs. Accountability is an unsolved problem so far