Introduction to PETS

194.144 Privacy-Enhancing Technologies

Dr. Markus Donko-Huber

Outline

Privacy Basics

What is Privacy?

Definitions

- *"The right to be left alone"* [Warren, Brandweis 1890]
- *"The right of the individual to decide what information about himself should be communicated to others and under what circumstances"* [Westin, 1970]

Different aspects

Important to understand different basic aspects of privacy.
The focus of this course are **technical** aspects.

- Socialogical
  impact of privacy on individuals
- Political and legal
  impact on society, companies

Socialogical Aspects

“I have nothing to hide“

Nothing to hide

“If you’ve got nothing to hide, you’ve got nothing to fear”

Google’s/Facebook’s position:

- *”If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.”* (Google’s Chairman Eric Schmidt, 2009)
- *”Privacy is no longer the social norm”* (Mark Zuckerberg, 2010)

Privacy is dead?

Private pictures on Facebook[1]

- pictures from Mark Zuckerberg leaked 2011
- security problem in reporting pictures
- private pictures were shown upon reporting
- even Mark Zuckerberg uses private pictures

[1] Forbes: Mark Zuckerbergs private photos exposed

Privacy is dead?

Privacy is dead?

'People are furious down here': Hundreds of protesters will amass at Mark Zuckerberg's Hawaiian wall

Alex Heath
27.01.2017, 01:05

TECH & SCIENCE

FACEBOOK CEO MARK ZUCKERBERG'S WALL PROVOKES HAWAII PROTESTS

BY ANTHONY CUTHBERTSON ON 1/27/17 AT 9:47 AM

EVERYDAY MONEY • REAL ESTATE

Mark Zuckerberg Bought Four Houses Just to Tear Them Down

Mark Zuckerberg Just Spent More Than $30 Million Buying 4 Neighboring Houses For Privacy

Alyson Shontell Oct. 11, 2013, 7:42 AM

Everyone needs privacy

- Physical privacy (curtains, doors)
- Health-related issues
- Work-related (e.g. unions)
- Political views

less privacy ==
more security?

Panopticism

- social theory by Foucault, *Discipline and Punish*
- idea: increased supervision leads to more security
- Panopticon = for supervision in prisons
  - subject is in constant visibility
  - self-censorship as consequence
  - operator in the tower has “anonymous power”

Panopticism

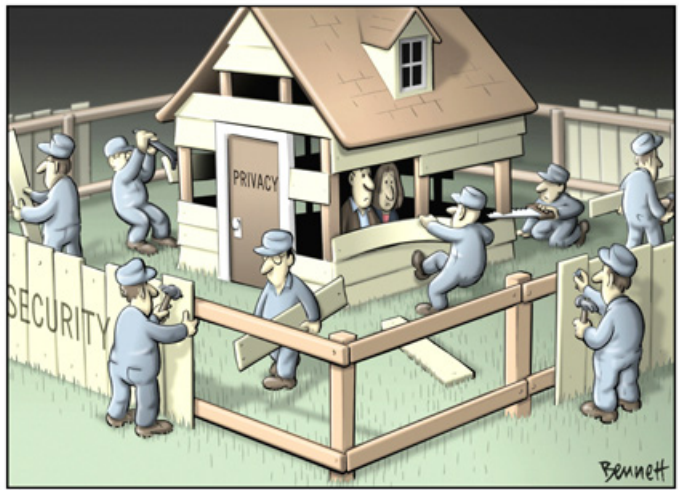
Figure: Presidio Modelo prison, Cuba (Wikimedia Commons)

Paternalism

"action that limits a person's or group's liberty or autonomy and is intended to promote their own good"

- seat belts, non-smoking regulations, ...
- ...but also social behavior: online gaming, shopping, religious practices, etc.

less privacy == more security?



Surveillance

- scope
  - **mass-surveillance**: “let’s collect location data of all mobile phones in our country in order to catch terrorists”
  - **targeted-surveillance**: “let’s wiretap people we suspect of planing a terror attack”
- Internet / phone surveillance, and CCTVs are common mass surveillance technologies

Facial Recognition Systems

Use of facial recognition systems

- Law-enforcement: identification of suspects, protesters
- Costumer profiling (age, gender, ...)
- Linking random people to their online profiles (e.g. FindFace[2])

"Experience how AI judges your face"
https://www.hownormalami.eu

[2] see: source

Facial Recognition Systems II

Challenges and Countermeasures

- Accuracy and potential racial bias
- Image cloaking with “Fawkes“

Targeted-Surveillance with Spyware

Offensive intrusion and surveillance

- Weapanized with zero-days for e.g. Android, iOS
- Hidden surveillance: location, messages, contacts etc.

Commercial offerings

- e.g. HackingTeam or NSO Group
- Government clients for combating crime and terrorism

Misuse of surveillance tech

Documented cases of abuse:

- video surveillance at Schwedenplatz
- Austria, 2005
- out of boredom they watched people in their homes[3]

NSA analysts stalked ex-partners:

- dupped LOVEINT[4]
- willful misconduct by NSA employees

[3] Wiener Verein hackt Polizeikamera: Der Spiegel

[4] LOVEINT: The Washington Post

Athens Olympics (2004)

The Athens Affair[5]:

- more then 100 mobile phones wiretapped
- rootkit was detected
- prime minister, mayor of Athens, journalists, opposition, military, ...
- lawful interception feature in Ericsson switches[6]
- Did not end well for the system administrator[7]

Recent incident in 2022[8]

[5] IEEE: The Athens Affair

[6] Wiki: Greek Wiretapping Case

[7] Death in Athens NSA Operation The Intercept, 2015

[8] Greek wiretapping scandal of 2022

Pegasus Project investigation (2020)

Forbidden Stories: Pegasus Project[9]:

- Pegasus is a popular spyware from NSO Group
- Leak of 50,000 targeted phone numbers
- Widespread misuse discovered
- Authoritarian governments spy on human rights activists, journalists and lawyers

Recommended documentary: Pegasus - Der Feind liest mit

[9] about the pegasus project

further reading

Privacy in classic literature

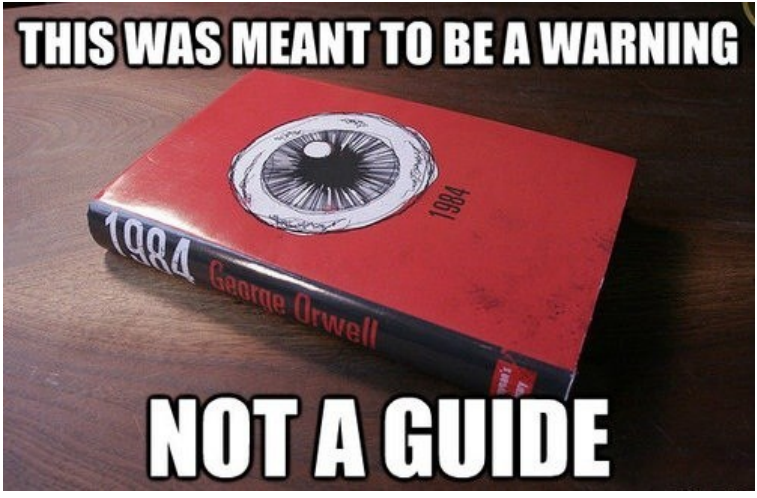
Orwell:

- Orwell's Nineteen Eighty-Four
- "Big brother"
- Telescreens

Kafka:

- Kafka's The Trial
- a person is arrested and prosecuted
- not knowing the nature of his crime
- surveillance states usually not transparent

1984


THIS WAS MEANT TO BE A WARNING
1984
1984 George Orwell
NOT A GUIDE

Further (online) material on privacy

Video:

- “Why privacy matters”
- TED Talk by Alessandro Acquisti, available here

Video 2:

- “How the NSA betrayed the world’s trust”
- TED Talk by Mikko Hypponen, available here

Book:

- Mark Elsberg “Zero”

Legal and Political Aspects

Privacy as a Universal Human Right

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence"

[Universal Declaration of Human Rights (UDHR)]

Figure: private cat

Legal: Article 8 of the European Convention on Human Rights

- *Everyone has the right to respect for his **private and family life**, his **home** and his **correspondence**.*
- *. . . except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

Legal: Data Retention Directive

- *Directive 2006/24/EC (2011 - 2014)*
  - citizens' telecommunication data
  - duration, number of phone calls, IP adresses, IMSI & IMEI, cell-IDs, ...
  - Germany and Czech Republic declared it unconstitutional in March 2011
  - April 2014: Court of Justice of the European Union declared the directive invalid
- Austria: Sicherheitspaket 2018 (targeted surveillance)
- Europe: Discussion for new data-retention (2019)

Legal: EU GDPR (DSGVO)

- *General Data Protection Regulation* [Regulation (EU) 2016/679]
- Data **breaches** need to be reported within 72 hours
- Right to **delete**, **export** data, marketing **opt-out**
- Privacy by Design and by Default
- Fines / Sanctions
  - Up to EUR 20 Million / 4% of global turnover
  - Enforced since 25th of May 2018

Legal: EU ePrivacy Regulation (2019)

- Revised draft published in September 2018[10]
- Regulate use of **web cookies and tracking**
- Ongoing disputes with ad tech lobby

[10] https://iapp.org

Political aspects

- Surveillance
  - Mass surveillance vs. targeted attacks[11]
  - Attacks against people, organizations, industry
  - Insights since Snowden revelations and hacked providers[12]
- Censorship
  - Hack and track down political opposition[13]
- Conformity (Panopticism/Paternalism)
  - Social Credit System[14] in China (since 2013): travel bans, social status, exclusion from school admissions …

[11] e.g. NSO Group, Candiru, HackingTeam, FinFisher

[12] e.g. Phineas Fisher

[13] 65 individuals targeted in Catalonia - Would you click?

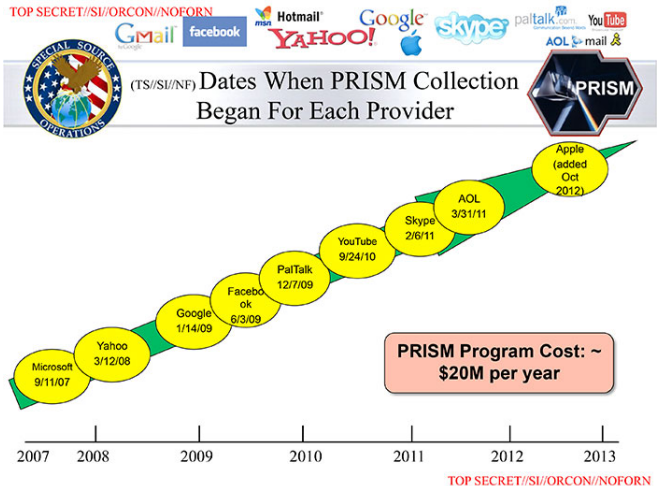
[14] Wiki: Social Credit System

Snowden Revelations

NSA revelations by Edward Snowden:

- Summer 2013
- information still not fully released
- Background information
  - “Citizen Four” by Laura Poitras
  - “Snowden” by Oliver Stone
- “The Intercept”, books, ...
- Glenn Greenwald, Barton Gellman, ...

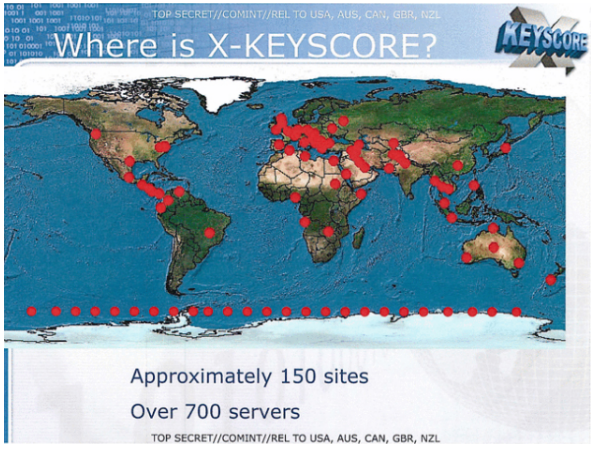
PRISM


TOP SECRET//SI//ORCON//NOFORN
Hotmail
Google
facebook
YAHOO!
skype
paltalk.com
YouTube
Gmail
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) Dates When PRISM Collection Began For Each Provider
PRISM
Microsoft 9/11/07
Yahoo 3/12/08
Google 1/14/09
Facebook 6/3/09
PalTalk 12/7/09
YouTube 9/24/10
Skype 2/6/11
AOL 3/31/11
Apple (added Oct 2012)
PRISM Program Cost: ~ $20M per year
2007
2008
2009
2010
2011
2012
2013
TOP SECRET//SI//ORCON//NOFORN

PRISM:

- targets data at rest
- allegedly direct access to data from Facebook, Apple, Google, Microsoft, AOL, Dropbox, Yahoo ...
- first story run by Glenn Greenwald, June 6 2013
- targeting internet communication
- Microsoft helped the NSA to circumvent its encryption e.g. the Outlook.com portal
- VoIP, emails, search queries, social interactions, files, ...

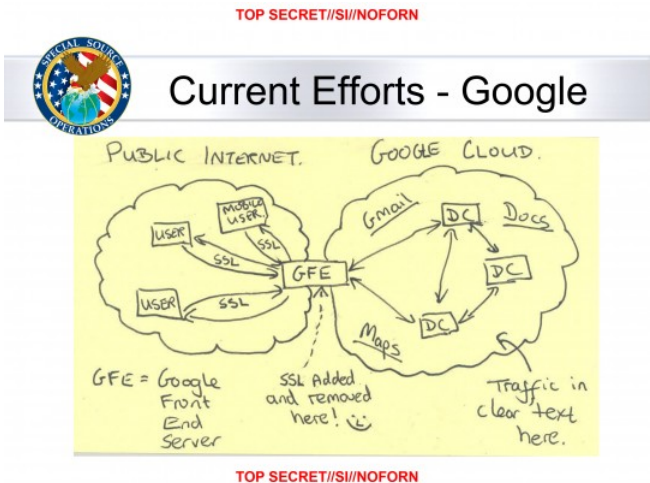
X-KEYSCORE


TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Where is X-KEYSCORE?
KEYSCORE
Approximately 150 sites
Over 700 servers
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

X-KEYSCORE:

- analytical database
- interface for various backends
- close to Internet backbones, passive in nature
- can trigger active attacks like QUANTUM attack-suite (FOXACID)
- read more here

SSL added and removed here …



MUSCULAR:

- operated by GCHQ
- targeting communication links between data centers
- Google and Yahoo!
- twice as many “selectors” as PRISM

Calls and Metadata ....

Source: Online here

Metadata

But it's just metadata?

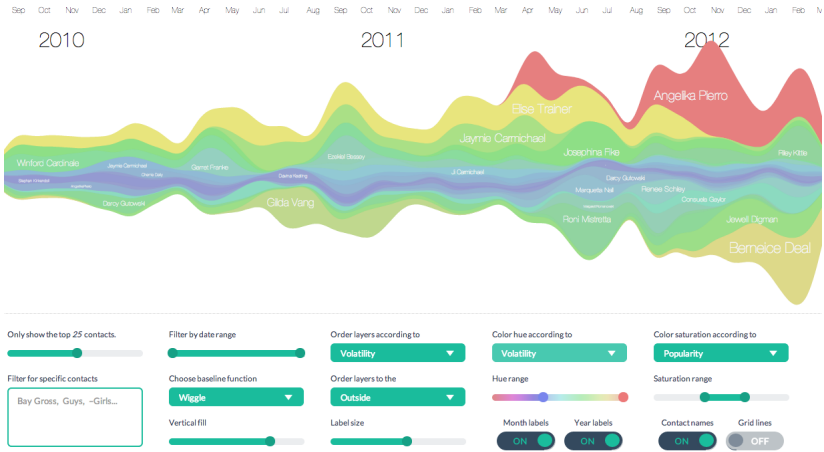
- who communicates with whom
- collected at humongous scale
- also, buffered for 30 days (TEMPORA)
- no direct access to content needed
- three degrees of separation

AND:

- people get killed based on metadata![15]
- personal health, political views, social graph, ...

[15] Gen. Michael Hayden: "We kill people based on metadata"

iPhone Metadata



Source: prismviz

Metaphone

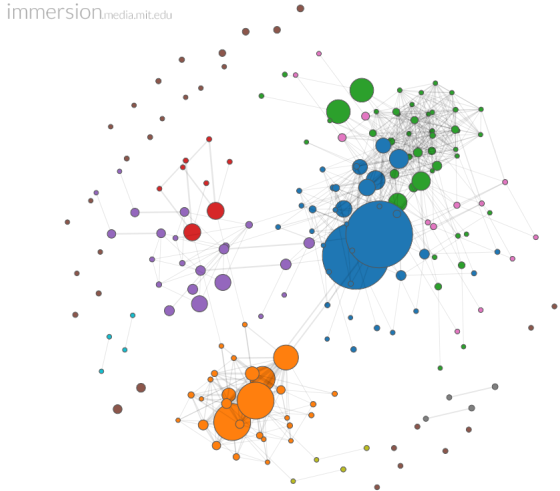
Other projects - Metaphone:

- Android app to visualize phone and sms data
- see this blogpost for details

Other projects - immersion:

- online at https://immersion.media.mit.edu/
- project of MIT MediaLabs
- visualization of email metadata (Gmail, Yahoo, MS Exchange)

Immersion



Social Snapshots

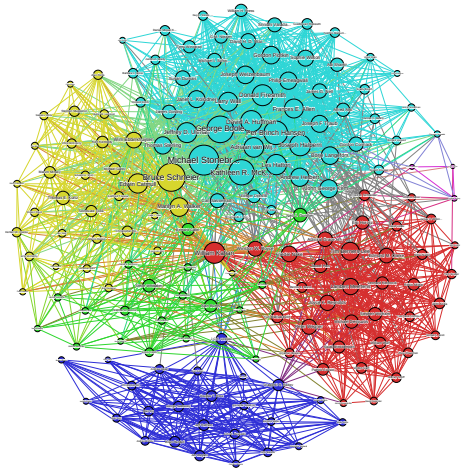
Other projects - SocialSnapshots:

- one of my prev. projects
- ~~get all Facebook content via the API~~[16]
- ~~get the graph of your social connections~~[17]
- Wolfram-Alpha has a similar feature

[16] Sourcecode available here

[17] Sourcecode available here

Social Graph



Snowden Leaks - so what?

”We already knew that NSA is spying . . . that is their job!” BUT

- mass surveillance vs. targeted information collection
- scale of surveillance
- 65 things we now know about NSA surveillance[18]
- a great timeline of the leaked info from 2016[19]

[18] See EFF

[19] Timeline by Business Insider

Are we doomed? Not really[20] ...

- Hide in the network: Use Tor and hidden services
- Encrypt your communications: Use TLS.
- Assume that while your computer can be compromised, it would take work and risk on the part of the NSA – so it probably isn't.
- Be suspicious of commercial encryption software, especially from large vendors.
- Try to use public-domain encryption that has to be compatible with other implementations.

[20] Source: Bruce Schneier, The Guardian, 2013

Technical Aspects

Privacy and Security (Engineering)

Privacy & Security

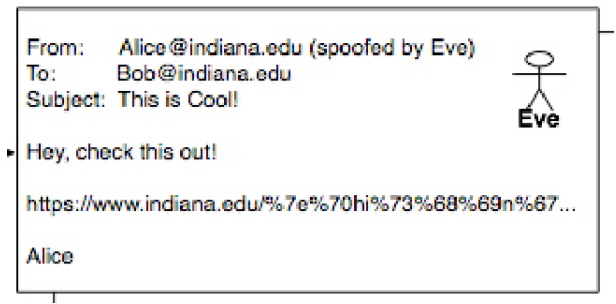
- Exploiting weak privacy for attacks
  - Social engineering, OSINT for attack preperation
- Security as a requirement for privacy
  - Companies, organizations must protect personal information
  - Privacy compliance requires adequate security measures (e.g. GDPR, CCPA)

Social Engineering

- human as weakest link
- social phishing [Jagatic et al.]
- context-aware spam [Brown et al.]
- identity-theft
- APTs, “advanced persistent threats”
- password questions

Social Phishing

- attack by Jagatic et al.
- additional information from social networks
- phishing success increased from 16 % to 72 %



Context-aware spam

- personal information from social networks
- way more successful [Brown et al.]

Hi [FIRSTNAME],
[SENDERNAME] ([SENDEREMAIL]) has sent you an online greeting card from BirthdayCards.com!

To pickup your card, please click on the following link:
http://www.birthdaycards.com/pickup?ID= A222-FHRE
(Link to attacker-controlled site)

If you are unable to click on the link above, please try cutting and pasting the URL into the address bar of your web browser. You may also go to our website at:
http://www.birthdaycards.com **(Link to attacker-controlled site)** and choose the "Pickup" option at the top of the page.
Your Pickup ID is: A222-FHRE

BirthdayCards.com - High Quality Greetings for All Occasions.
If you have any other questions or problems, please visit our support page at:
http://www.birthdaycards.com/support.momd

Social (Network) Engineering

“Profile-cloning” attacks[21]:

- create second account e.g. Facebook, and invite friends of target

“Cross-Network-Cloning ”

- victim on Facebook, but not LinkedIn)

User profiling:

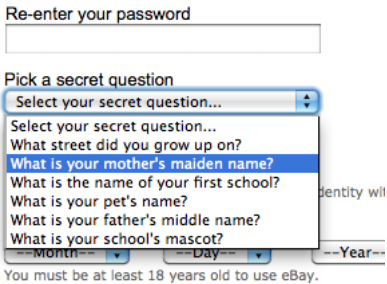
- validate email addresses using social networks
- spammers can collect additional information

[21] Leyla Bilge et al., “All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks”, WWW 2009

Account Takeover: Secret Questions

"Secret questions" to regain control of accounts:

- can be answered using social networks



Account Takeovers nowadays

- “Mat Honan hack” , see here
  - Attackers wanted to get @mat handle
  - Exploited chain of support issues with public information
- SIM swap scams
  - Attackers gather phone number and personal information
  - Attackers request port of phone number to “new” SIM cards
  - control of phone number == control of all online accounts (SMS as MFA fallback)
- Voice phishing (vishing)
- Impersonate legitimate sources based on OSINT

Privacy Enhancing Technologies

What are PETs?

"Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by ***eliminating or minimizing personal data*** *thereby preventing unnecessary or unwanted processing of personal data,* ***without the loss of the functionality*** *of the information system."*

[van Blarkom, Borking & Olk 2003]

How we understand PETs . . .

- focus on **online services**
- methods and tools that work for **specific threat** model
- wtf is “NSA safe”, anyway?
- similar to “digital ” curtains
- defense in depth

What are PETs?

Mechanism of control:

- about personal information
- in transit, at rest
- applied cryptography
- OTR, TLS, ZRTP, HSTS, GPG, . . . OMG, WTF

What are PETs?

Mechanism of anonymity:

- no information on who did something
- example: public elections
- weaker form is pseudonymity (use of nick names)

What are PETs?

Mechanism of unlinkability:

- dates, times, IPs, locations
- example: Wikipedia with pseudonyms (Kobuk: Eva Dichand)
- tools: Tor, Remailer, Ricochet

PETS Origins: Cypherpunks

Cypherpunks = cipher + cyberpunks

- until the 70s cryptography was for military and secret services
- RSA & DES changed that, were publicly known
- David Chaum inspired the cypherpunk movement (80s)
- math, cryptography, computer science
- more than 2000 members on the mailing list (peak)
- discussions on privacy and control of information

Cypherpunk's Manifesto

Privacy is necessary for an open society in the electronic age. . . . We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy . . . We must defend our own privacy if we expect to have any.
. . . Cypherpunks write code. We know that someone has to write software to defend privacy, and . . . we're going to write it.

[Hughes, Eric (1993), A Cypherpunk's Manifesto]

PETS origins: Cypherpunks

Cryptoparty

- *"Party like it's December 31st, 1983"*
- current successor of the cypherpunk movement
- August 2012
- free workshops on cryptography, Tor, ...
- worldwide, e.g., Hawaii with Snowden in December 2012
- Austria: `https://cryptoparty.at`

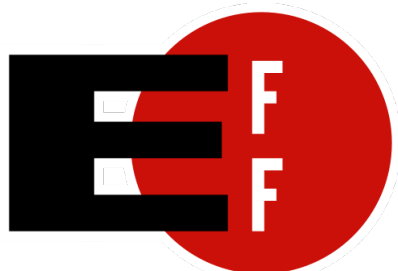
PETS origins: EFF

Electronic Frontier Foundation (EFF):

- NGO based in the US
- founded 1990 as answer to lawsuits against Hacker
- defenders of information freedom
- provide technical and legal support
  - Bernstein vs. United States (1995)
  - EFF DES cracker (1999)

current projects:

- Privacy Badger
- Lets' encrypt




#NSA KILLED MY INTERNET
NOW I HAVE TO BUILD A GNU ONE

Summary

Summary

To conclude

- import to understand various privacy aspects
- ~~“nothing to hide”~~ everybody has something to hide
- privacy is a fundamental human right
- Snowden: mass surveillance vs. targeted surveillance
- Relationship of Privacy vs. Security
- PETs are technological means to protect privacy