Protecting Privacy and Freedom Online with FOSS

Presented By Steven Arbitman
Starbits Studios, Inc.
www.starbits.com
For FOSSCON 2012

Who Has Privacy?

Criminals, Major Corporations, Governments, basically everyone but NOT YOU!

Good news: Findings reveal that 91 percent of U.S. online adults worry about their privacy.

Bad news: it may be worse than you think.

Good news: - you can be private, for free, with little effort and no technical knowledge.

Why Bother? I have nothing to hide.

- Postcards or Envelopes - Which would you use?

If You Have Nothing To Hide

From Saturday Morning Breakfast Cereal, Zach Weiner

http://www.smbc-comics.com/index.php?db=comics&id=2434

Who Is Watching?

- Criminals
- Cyber-activists
- Corporations
- Governments

"It will feel like data has a life of its own. With the massive amount of sensors we have littering our lives and landscapes, we'll have information spewing from everywhere. Our cars, our buildings, and even our bodies will expel an exhaust of data, information, and 1s and 0s at an incredible volume."
The Secret Life of Data in the Year 2020 By Brian David Johnson

They Know Where You Are - Geolocation

- Federal, state, and local law enforcement agencies have made over 1.3 million demands for user cell phone data in the last year, "seeking text messages, caller locations and other information." The New York Times called the new findings proof of "an explosion in cellphone surveillance"
- Civilian GPS tracking $150 - $500
- Solutions? Detectors, Wave Bubble, GPS Spoofers
- EZ-Pass, traffic cameras, drone aircraft, RFID

Privacy Invasions - Examples

- Comcast blocking file sharing
- Target and teen pregnancy – store cards
- Lower Merion – laptop cameras
- Government Invasions of Privacy

The NSA

- AT&T “Secret Room” revealed in 2006
- Former NSA employes William E. Binney, Thomas A. Drake, and J. Kirk Wiebe - “widespread mass illegal surveillance of ordinary people”.
- “Neither the Constitution nor federal law allow the government to collect massive amounts of communications and data of innocent Americans and fish around in it in case it might find something interesting. This kind of power is too easily abused. ... whistleblowers have come forward to help end this massive spying program." (source: eff.org)

Cell Phones and the FBI

- Network spoofing

- Cell phones can be activated as surveillance microphones: The technique is called a "roving bug," and was approved by top U.S. Department of Justice officials for use against members of a New York organized crime family who were wary of conventional surveillance techniques such as tailing a suspect or wiretapping him.

Drone Aircraft - UAVs

One North Carolina county is using a UAV equipped with low-light and infrared cameras to keep watch on its citizens. The aircraft has been dispatched to monitor gatherings of motorcycle riders at the Gaston County fairgrounds from just a few hundred feet in the air--close enough to identify faces--and many more uses, such as the aerial detection of marijuana fields, are planned.

http://news.cnet.com/Drone-aircraft-may-prowl-U.S.-skies/2100-11746_3-6055658.html

http://articles.latimes.com/2011/dec/10/nation/la-na-drone-arrest-20111211

https://www.eff.org/deeplinks/2012/06/federal-government-moves-forward-drone-programs-despite-poor-planning-and-lack

Cars, Pacemakers and More

Everything wireless is vulnerable –
and everything is wireless

- Pacemakers
- Insulin pumps
- Cars
- Garage Door Openers
- Baby monitors
- Your brain?

http://news.yahoo.com/blogs/technology-blog/5-things-probably-didn-t-know-could-hacked-174330493.html

The Law

- Laws that are out of date
- Laws that are not in your interest

Reasonable expectation of privacy:
phone booth = private, cell phone in open = public

home = private, workplace = public, internet cafe = public

Emails: addresses - IPs are PUBLIC

Email content - private in transmission, semi-private after receipt.

This Email is Confidential

Our company accepts no liability for the content of this email, or for the consequences of any actions taken on the basis of the information provided. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

Notice: Unless you are named "Arnold P. Fasnock", you may read only the "odd numbered words" (every other word beginning with the first) of the message above. If you have violated that, then you hereby owe the sender $10 for each even numbered word you have read.
http://goldmark.org/jeff/stupid-disclaimers/

New Data Privacy Laws

- http://www.informationshield.com/usprivacylaws.html
- Companies who do E-commerce in Nevada or Massachusetts, or with customers in these states, are now subject to data privacy laws requiring not only notification of data breaches — but encryption of stored or transmitted personal data.
  http://arborlaw.biz/blog/2009/02/25/new-nevada-massachusetts-data-privacy-laws-impact-internet-businesses/
- CISPA (the Cyber Intelligence Sharing & Protection Act)

What to do:
End to End Security

- From your keystrokes across the internet to and past your destination.
- Remember the human element - recipient can release the information also.
- Your PC is vulnerable to search and seizure (and theft).

Why You Want Open Source

- Code is reviewed - no "backdoors"
  Bugs are found and fixed quicker than proprietary
- Free Software (GPL), Open Source Software and "free" software.
- Counter-Example: Electronic Voting Software

AntiVirus and Firewalls - Part of the Solution

- Keyloggers
- AntiVirus Software – clamwin, Avira, AVG
- Firewalls – netdefender, ZoneAlarm, Comodo

Encryption – Another Part of the Solution

- Public Key Encryption – key pairs
  Don't give away how to decrypt
- Security Certificates – Are you really who you say you are?
  But Certificate Authorities have been hacked.
- Kerckhoffs' principle: Put all your secrecy into the key and none into the cryptographic algorithm. The key is unique and easily changeable; the algorithm is system-wide and much more likely to become public. In fact, algorithms are deliberately published so that they get analyzed broadly.
  https://www.schneier.com/blog/archives/2012/06/on_securing_pot.html
- Is it good enough? Jan. 2000, export controls relaxed.

Passwords and Problems

- Your dog's name and birthday won't do it anymore. The 10 most common passcodes used by iPhone users accounted for 15 percent of all the passwords that were analyzed. - Daniel Amitay

- How to make strong passwords
  let me in -> L3t^m3^1n!!!

- https://www.grc.com/haystack.htm
  http://world.std.com/~reinhold/diceware.html

- How to remember strong passwords
  PasswordSafe & KeePass

Protection At Your PC
Part 1 -Tempests and Drones

Protection At Your PC
Part 2 – Disk Encryption

- True Crypt http://www.truecrypt.org/
- Good beginner instructions
- “Plausible Deniability”

Email Privacy

- Anonymous Email
  http://www.guerrillamail.com/
- Encrypted Email
  https://riseup.net/en
  https://www.hushmail.com/
- Use different email identities
  http://www.spokeo.com - tracks by email address

Protection Online
They Know Where You Are

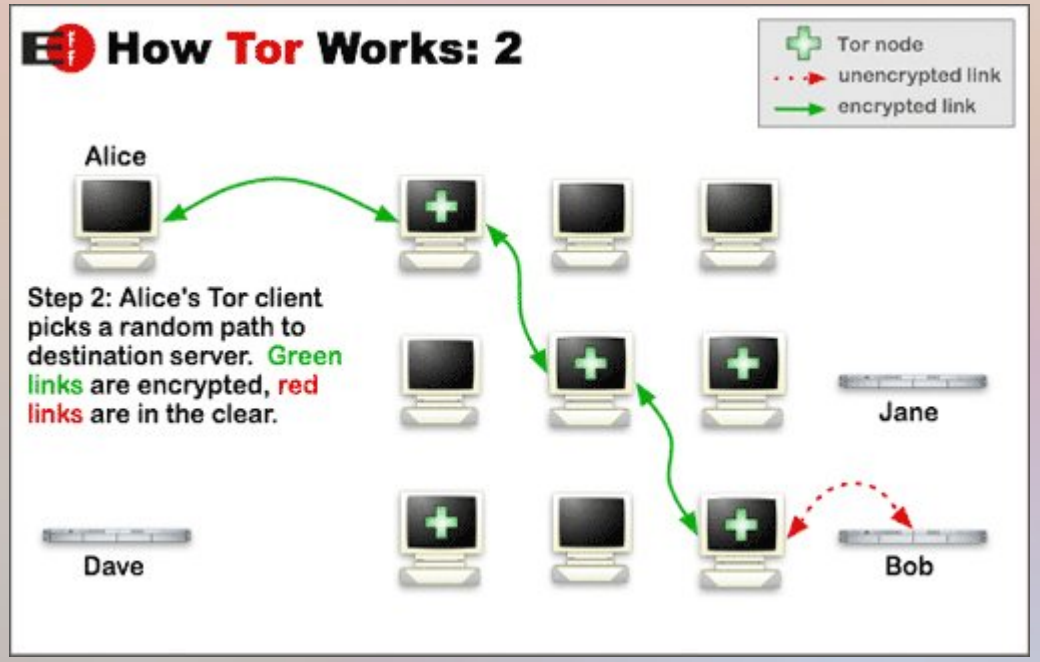
- Your IP Address:
  71.175.129.147
  pool-71-175-129-147.phlapa.east.verizon.net
- Solution: Virtual Private Network or Proxy or Tor
  70.32.45.243
  prod04.s.ewr.fullmeshnetworks.com
- DNS - turns names into IP addresses
- https://www.opendns.com/

Tunneling - Virtual Private Networks

- Encrypted from your PC to somewhere else in the world
- Security in hotels and airports
- OpenVPN – open source VPN software
- Faster than Tor
- Relies on the third-party VPN provider

Browser Privacy
Part 1 - TOR

- Top of the line – encrypted right at your PC, emerging in the clear somewhere else in the world
- Slow. no Flash or PDFs
- Open Source, sponsored in part by DARPA
- www.torproject.org



Browser Privacy
Part 2 – Tracking Cookies

- Data from a website saved on your PC
- Session, persistent, 3rd party, zombie
- DNT+ Firefox add-on

Part 3 – HTTPS Everywhere

- Firefox and Chrome add-on
  https://www.eff.org/https-everywhere

Chat – Off The Record (OTR)

- Pidgin-otr http://www.cypherpunks.ca/otr/
- https://crypto.cat/
- Phone texting apps (from Wikipedia) "TextSecure", "Gibberbot"
- "ChatSecure", a free open-source iPhone application (in early development)
- "Beem", a free, GPL-licensed Jabber/XMPP client on Android.

Protection on the Phone

- Encrypted VOIP - Zfone http://zfone.com works on Magic Jack but not Skype
- Skype Security Claims - not open source but independently verified – but keys are probably kept for Govt. use.
- https://guardianproject.info/ - for Android phones

The Problem Of Money

- The need for electronic cash
- Bitcoin: http://bitcoin.org/

Bitcoin is an **experimental** *(emphasis added)* new digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate with no central authority: managing transactions and issuing money are carried out collectively by the network. Bitcoin is also the name of the open source software which enables the use of this currency. The software is a community-driven open source project.

The Future – Coming Soon?

- Freedom Box
  http://freedomboxfoundation.org/
- Commotion Wireless Project
  https://code.commotionwireless.net
- Project Byzantium
  http://project-byzantium.org

Fear of Repression Spurs Scholars and Activists to Build Alternate Internets: http://chronicle.com/article/Fear-of-Repression-Spurs/129049/

Additional References

- The Cuckoo's Egg, Cliff Stoll
- Protecting Your Internet Identity, Claypoole & Payton
- Gibson Research Corp.http://www.grc.com/intro.htm
- The Electronic Frontier Foundation: https://www.eff.org/
- Electronic Privacy Information Center: http://epic.org/
- Ted: http://www.ted.com/talks/rick_falkvinge_i_am_a_pirate.html http://www.ted.com/talks/james_stavridis_how_nato_s_supreme
- Nova: "The Spy Factory"

Conclusion - What I Use

- Password Safe
- Antivirus and firewall and Open DNS
- VPN
- HTTPS everywhere and DNT+
- Anonymous email and hushmail
- Separate Identities – still working on this

"Any society that would give up a little liberty to gain a little security will deserve neither and lose both."
Benjamin Franklin