CAN YOU PROTECT YOURSELF IN CYBERSPACE?

REALLY????
WHO WANTS THE LIVE IN A GLASS HOUSE?
WHO WANTS THE LIVE IN THIS FUTURE?
CYBER SPACE: A Dangerous Place?
CYBER SPACE: USA’s Infrastructure—Partial
CYBER SPACE:
China’s Infrastructure
SCOPE OF CYBER SPACE
VULNARABILITIES OF CYBER SPACE:
Instantaneous Action at a Distance

NORSE
VULNARABILITES OF CYBER SPACE:
Asymmetries of Cyber Space

NORSE
VULNARABILITIES OF CYBER SPACE: Anonymity

“On the Internet, nobody knows you’re a dog.”
VULNARABILITIES OF CYBER SPACE:
Lack of Borders
VULNARABILITIES OF CYBER SPACE: Difficulty of Distinction
PRIVACY: Who is after your private Data

“Every time you pick up the phone, dial a number, write an email, make a purchase, travel on the bus carrying a cell phone, swipe a card somewhere, you leave a trace and the government has decided that it’s a good idea to collect it all, everything, even if you’ve never been suspected of any crime.”
PRIVACY: Who is after your private Data

CORPORATIONS

WE COOPERATE WITH CORPORATE SURVEILLANCE BECAUSE IT PROMISES US CONVENIENCE, AND WE SUBMIT TO GOVERNMENT SURVAILLANCE BECAUSE IT PROMISES US PROTECTION.
PRIVACY: Who is after your private Data
CYBER CRIMINALS
PRIVACY: HOW CAN YOU PROTECT YOURSELF

HDD ENCRYPTION - Bit Locker, PGP
PRIVACY: HOW CAN YOU PROTECT YOURSELF
FILE ENCRYPTION- EFS, FILEVAULT (MAC)
PRIVACY: HOW CAN YOU PROTECT YOURSELF

SECURE E-MAIL: S-MIME, PGP, MAILVELOPE, GMAIL-STAKE

Is your email secure?
“ThrowAwayMail.com”
Provides a randomly generated email.

“10 Minute Mail”
Provides a randomly generated email that shuts down after 10 minutes.
Allows you to see emails sent to the address (ex: account verification emails).

“SMS Receive Free”
Provides phone numbers that can be used for verification codes, etc.
Each number has its own page, where you can see all messages sent to that number.
PRIVACY: HOW CAN YOU PROTECT YOURSELF
ANTIVIRUS-MALWARE-SPYWARE-FIREWALLS
PRIVACY: HOW CAN YOU PROTECT YOURSELF

PASSWORD MANAGEMENT - LastPass - Keeper
PRIVACY: HOW CAN YOU PROTECT YOURSELF
DELETING DATA - ERASER
PRIVACY: HOW CAN YOU PROTECT YOURSELF
SECURE CLOUD STORAGE - SPIDEROAK
PRIVACY: HOW CAN YOU PROTECT YOURSELF
SECURE PRIVATE BROWSING - TOR

Tor

Anonymity Online
Protect your privacy. Defend yourself against network surveillance and traffic analysis.

Download Tor

What is Tor?
Tor is free software and an open network that helps you defend against a form of network.

Why Anonymity Matters
Tor protects you by bouncing your

Home About Tor Documentation
PRIVACY: HOW CAN YOU PROTECT YOURSELF
SECURE PRIVATE SEARCH ENGINE - DUCK DUCK GO
PRIVACY: HOW CAN YOU PROTECT YOURSELF

SECURE WIRELESS CONNECTION - WPA2
THE CONSTITUTION AND CYBERSPACE

FOURTH AMENDMENT

The Fourth Amendment of the U.S. Constitution provides, "[t]he 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."

The ultimate goal of this provision is to protect people’s right to privacy and freedom from arbitrary governmental intrusions.

The protection under the Fourth Amendment can be waived if one voluntarily consents to or does not object to evidence collected during a warrantless search or seizure.

Private intrusions not acting in the color of governmental authority are exempted from the Fourth Amendment.
DATA COLLECTED BY APPS: EXAMPLE

Take pictures and videos
Record audio
Location information (Approximate, Precise)
Read your Web bookmarks and history
Modify or delete contents of your SD card
Control NFC
Add or remove accounts
Change your audio settings
Read sync settings
Install shortcuts
Access Mobile Device Management (MDM) content providers
GDPR: Global Data Privacy Regulations

- Increased Territorial Scope
- Penalties up to 4% revenue or 20 Million Euro
- Consent must be intelligible and accessible
- Breach notification 72 hours
- Right of access – free copy
- Right to be forgotten
- Data Portability
- Privacy By Design
- Data Protection Officers requirements
GDPR: Global Data Privacy Regulations

Companies Must Also…

1. Tell individuals how their personal data will be used
2. Grant individuals access to correct or erase their personal data upon request
3. Comply with requests from individuals to stop using their personal data for marketing
4. Keep personal data secure
5. Make sure staff are appropriately trained in the care and handling of personal data
6. Put data processing agreements in place to ensure third party vendors follow the same protective rules
7. Notify regulators and/or affected individuals in the event of a serious data breach (usually within 72 hours)
8. Limit transfers of personal data out of the European Economic Area to only those that comply with EU international data transfer rules
9. Build privacy compliance into product, software and services design, processing tools and system development
CCPA: California Consumer Privacy Act

- Right to know all data collected by a business on you.
- Right to say NO to the sale of your information.
- Right to DELETE your data.
- Right to be informed of what categories of data will be collected about you prior to its collection, and to be informed of any changes to this collection.
- Mandated opt-in before sale of children’s information (under the age of 16).
- Right to know the categories of third parties with whom your data is shared.
- Right to know the categories of sources of information from whom your data was acquired.
- Right to know the business or commercial purpose of collecting your information.
- Enforcement by the Attorney General of the State of California.
- Private right of action when companies breach your data, to make sure these companies keep your information safe.
<table>
<thead>
<tr>
<th></th>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basis for consent</strong></td>
<td>Opt in</td>
<td>Opt out</td>
</tr>
<tr>
<td><strong>Who it applies to</strong></td>
<td>Any organisation holding personal data on EU citizens</td>
<td>For-profit entities that process personal data of California residents and either:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Do $24 million in annual revenue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Hold the personal data of 50,000 people, households, or devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Do at least half of their revenue in the sale of personal data.</td>
</tr>
<tr>
<td><strong>Rights for individuals</strong></td>
<td>Access to data being held, right to erasure, correction, object to automated processing, Right to notification if there is a data breach.</td>
<td>Right to disclosure and objection relating to who data is being sold to, no discrimination if individual objects to data sold. Right of access to data being held. Right to know how personal data is being used. Right to know who data has been provided to.</td>
</tr>
<tr>
<td><strong>When does it come into force</strong></td>
<td>May 25, 2018</td>
<td>Jan 1, 2020</td>
</tr>
<tr>
<td><strong>Financial Penalties</strong></td>
<td>4% of turnover or €20m (whichever is greater)</td>
<td>$7,500 per violation. $750 or actual damages for each individual, whichever is greater</td>
</tr>
<tr>
<td><strong>Time allowed to respond to a request</strong></td>
<td>1 month</td>
<td>45 days</td>
</tr>
</tbody>
</table>
“I AM REGULARLY ASKED WHAT THE AVERAGE INTERNET USER CAN DO TO ENSURE HIS SECURITY. MY FIRST ANSWER IS USUALLY ‘NOTHING; YOU’RE SCREWED’.”

BRUCE SCHNEIER