Electronic Frontiers Georgia
Protecting and Promoting Online Civil Liberties

web: https://ef-georgia.org
email: info@ef-georgia.org

Key Policy Positions

Government should be transparent / open to public feedback

Property rights should extend to technology
- Right to repair
- Right to reverse engineer (disability access, security research, education, etc.)
- Right to to make copies for backup
- see DMCA (Digital Millennium Copyright Act)

Copyrights
- Copyrights should have reasonable limits, then should go into public domain as originally intended

Patents
- Companies, individuals, universities, and government divisions should use their patents for useful products and services, not lawsuits (patent trolling)
- Possible idea: “Put it in play” requirement – patent must be put to use in a certain amount of time or should expire

Encryption
- Strong Encryption should not be a crime but should be defended, privacy is an important part of security and freedom - especially important to minorities and “at risk” populations
- Encryption is a cornerstone of finance, business transactions, health care - there is no way to “weaken” or “back door” encryption without leaving it wide open (“A back door for one is a back door for all”)
- see Apple v. FBI

Network Neutrality / Title II & Internet Governance
- Congress should take an active role and not leave it up to regulatory authorities to define policy for Internet governance
- Mozilla Poll: 76% of Americans across the aisle agree on fundamentals of Network Neutrality
- Equal access, no preference, discrimination or throttling based on content
- Broadband customers should have the right to opt-out of data collection (snooping), tracking (cookies), and customized advertising
- Citizens have the right to control information about themselves without onerous processes (re: data brokers)
- Users should have the right to be anonymous online
- Students/parents should have control of their data and can opt-out
- see Network Neutrality/Title II and CRA SJ34

FOSS – Free and/or Open Source Software
- Schools and Governments should encourage but not require OpenSource software for its security, cost, and educational value
- Voting software should be OpenSource, secure, audited, and kept up-to-date

Work

- Limited Non-compete agreements
- Should not allow biometric or medical data to impact employment opportunities

Surveillance Concerns (Police, TSA, Federal Bureaus)

Items that need more oversight and transparency to citizens:

- Biometric Collection
- Stingrays
- Mass CCTV / Facial Recognition / License Plate scanners
- Body Scanners
- Shotspotter
- Persistent Surveillance Systems
- Drones
- Security organizations shouldn't be stockpiling "0-Day exploits", as has been witnessed recently, this can lead to massive vulnerabilities
- Legal framework for monitoring ads and signage that sniff WiFi traffic to produce more targeted ads - need opt-outs, or honoring a Do-Not-Track request
- see Section 702 of FISA Act

Legislation and court cases that have had an impact on civil rights from technology standpoint *:

- Apple v. FBI
- CRA SJ34
- DMCA (Digital Millennium Copyright Act)
- GA HB-509 (Internet Blocking Act) - this is a state-level act, but it's not unheard of that something like this might also appear at the Federal level
- FISA Act, Section 702 allows Americans to be swept up in bulk data collection
- Miller v. ACLU
- Network Neutrality / Title II designation
- PATRIOT Act
- SOPA (Stop Online Piracy Act) / PIPA (Protect IP Act) - neither passed, but will likely come up again in another incarnation
- Wassenaar Arrangement

* Technology specialists who are politically active are concerned about these.