Glossary of Technology Policy Terms

- **Big Data:** Big data is the collection and analysis of large and complex data sets. This term is often described by the "Three V's" – volume, variety, and velocity. These qualities are important to understanding that this term not only applies to large data sets collected by one entity, but also combined data from multiple sources and the speed and quality of analysis it undergoes. Government agencies and businesses collect data from multiple sources, including: social media profiles, online comments and forum posts, computer and mobile device log files, cloud applications, and archived documents such as insurance forms and customer correspondence.

- **Biometrics:** Technology that identifies you based on your biological or behavioral traits (e.g. fingerprinting, facial recognition, genetic testing, or iris scanning). It is often used for security purposes but can also be used for surveillance.

- **Bulk Collection:** The government's practice of collecting massive amounts of data belonging to large groups of people in a generally indiscriminate manner. The National Security Agency intercepts over a billion people's telephone and Internet communications worldwide. Advocates are concerned about the amount of data collected and how the government uses this data.

- **Cybersecurity:** Measures taken to protect the security of computers and computer networks.

- **Data security:** Measures taken to protect the confidentiality, integrity, and availability of data.

- **Do Not Track:** A technical Web standard maintained by the World Wide Web Consortium; a feature in certain web browsers that allows users to let websites know that they would like to opt-out of third-party tracking. Third party companies collect web users' personal information and online activities for a variety of purposes, including behavioral advertising.

- **Fair Use:** Doctrine in American copyright law that permits limited use of copyrighted material. People using copyrighted materials for parody, news reporting or research often do not have to acquire permission from the rights holders.

- **Federal Communications Commission (FCC):** An independent U.S. government agency overseen by Congress that regulates interstate and international communications by radio, television, wire, satellite and cable.

- **Federal Trade Commission (FTC):** An independent U.S. government agency that protects consumers and eliminates anticompetitive business practices.

- **Section 702 of the FISA Amendments Act (2008):** Authorizes surveillance of people believed to be located outside the U.S. who are not U.S. citizens.

- **Gag Orders:** An order from courts or government agencies that restricts recipient companies from sharing information with the public or third parties.

- **Intermediary Liability:** When private companies are held responsible for what their users say and do online. In the U.S., there are strong protections for intermediaries from liability for their users' speech. Holding intermediaries legally responsible for what their users post can be used by governments to suppress dissent and limit intermediaries' willingness to host lawful speech.

- **International Telecommunications Union (ITU):** This is the United Nations' specialized agency for information and communication technologies. They allocate global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies seamlessly interconnect, and work to improve access to technologies in underserved communities worldwide.

- **Internet Corporation for Assigned Names and Numbers (ICANN):** ICANN is the nonprofit organization that coordinates the Internet's global domain name and addressing system.

- **Internet of Things:** Chips, transmitters, sensors, and other networking components placed in real-world objects or animals that can transmit data for a network. Examples include a heart monitor implant, a farm animal with a biochip transponder, or home appliances that can be programmed to learn your preferences and can be controlled remotely.

- **Metadata:** Metadata – technically, data about data – provides information about the records created or stored by a computer or telecommunications device. It can include how the data was created, the purpose of the data, the time and date the data was created, the creator or author of the data, numbers dialed to or from a device, and the location on a computer network where the data was created.

- **National Security Administration (NSA):** The U.S. intelligence agency responsible for global monitoring, collection, decoding, translation and analysis of information and data for foreign intelligence and counterintelligence purposes.

- **National Security Letters (NSL):** The FBI can issue an NSL to collect bank, telephone company, and Internet Service Provider customer records. Companies are required to comply with NSL requests and are prohibited by a gag order from telling customers when they receive these letters.

- **National Telecommunications and Information Association (NTIA):** An executive branch agency within the Department of Commerce that advises the president on telecommunication and Internet policy issues.

- **Net Neutrality:** The principle that Internet Service Providers and governments should treat all data on the Internet equally, by not prioritizing network traffic or charging different prices.

- **Online Behavioral Advertising (OBA):** Companies collect information about a person's online activity and use it to tailor ads or content.

- **Privacy by Design:** An approach to engineering, design or business plans that takes user privacy into account from the beginning and embeds it throughout the whole product development process.

- **Privacy Policy:** A statement or legal document that discloses the ways a party gathers, uses, discloses and manages a customer or client's data.

- **Right to be Forgotten:** The idea that an individual has the right to remove public information about themselves from the Internet, or to petition search engines not to list certain links to publicly available information in search results. Following a ruling from the Court of Justice for the European Union, the scope of this right is being explored in Europe, but faces skepticism in the United States because of its conflict with First Amendment principles.

- **Safe Harbor:** The data transfer agreement between the U.S. and EU recently struck down in the *Schrems* decision.

- **Section 512 of the Copyright Act (Safe Harbor):** A provision of The Digital Millennium Copyright Act which protects Internet Service Providers from the consequences of their users' actions, such as copyright infringement.

- **Section 215 of the Patriot Act:** Allows the government to obtain secret court orders to collect "tangible things" that could be relevant to a government investigation, such as books, records, papers and documents.

- **Subpoena:** When a prosecutor or government agency requires someone to testify or produce evidence - typically without seeking approval from a neutral third party like a judge.

- **Warrant:** A document issued by a judicial or government official authorizing the police or some other body to make an arrest or search premises.

- **Upstream Collection:** A term to describe the NSA's tactic for intercepting telephone and Internet traffic as it flows through major Internet cables and switches.

Legislation

Privacy Protection

Fair Credit Reporting Act (FCRA):
The FCRA was enacted in 1970 to promote accuracy, fairness and the privacy of personal information assembled by Credit Reporting Agencies, including requiring consumer protections for credit reports, consumer investigatory reports and employment background checks. Typically, consumer credit reports contain information on financial accounts, and include credit card balances and mortgage information. In addition to compiling traditional consumer credit reports, companies are now also creating social media reports, which are supplied to employers as part of employment screenings. In May 2011 the FTC confirmed that employers must comply with the requirements of FCRA when using public information furnished by Internet and social media background screening services.

Family Educational Rights and Privacy Act (FERPA):
This law was enacted in 1974 and protects the privacy of student education records. It gives parents the right to review a student's educational records and request corrections when the parent believes records are inaccurate or misleading. The law also requires, with a few exceptions, a school to have written permission from a parent before releasing a student's educational record to other parties.

Privacy Act of 1974:
The Privacy Act of 1974 requires government agencies to show people any records kept on them. It also requires government agencies to follow "fair information practices" when gathering and handling personal data and places restrictions on how agencies can share an individual's data with other people and agencies. It allows individuals to sue the government for violating these provisions.

Electronic Communications Privacy Act (ECPA):
ECPA was passed in 1986 to expand and revise federal wiretapping and electronic eavesdropping provisions. It was envisioned to create "a fair balance between the privacy expectations of citizens and

the legitimate needs of law enforcement," but it allows law enforcement warrantless access to any email after 180 days.

Video Privacy Protection Act:
Congress passed the Video Privacy Protection Act of 1988 to prevent the disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual material." The Act is not often invoked, but stands as one of the strongest protections of consumer privacy against a specific form of data collection.

Health Insurance Portability and Accountability Act (HIPAA):
HIPAA regulates when and how health information about individuals in the United States may be disclosed. The law offers some rights to patients, such as the ability to view and correct medical records, but its capacity to protect disclosures of patient medical information is limited, as the law only applies to health care providers, health plans, healthcare clearinghouses, and relevant business associates of these entities. While the law covers health information technology and electronic healthcare records, it does not apply to many entities that collect and use health information from individuals, such as mobile applications, wearable device companies, or genetic testing services. When non-HIPAA covered entities collect and use personal health information for internal purposes like research and development, these activities are also unregulated but they may be informed by laws such as the Common Rule, which sets ethical guidelines for how government-funded entities may gather and use information from human subjects. Ethical considerations should be a part of any use of data generated by human subjects, including the users of health apps or devices. Though the Common Rule only applies to federally-funded research, companies may find the law's detailed ethical guidance useful, including ways of obtaining and documenting informed consent and regulations on implementing special protections for data from minors and/or the disabled.

Children's Online Privacy Protection Act (COPPA):
COPPA was enacted in 1998 to regulate online data collection from children under the age of 13. It requires websites to post clear and comprehensive online privacy policies and get consent from parents before collecting children's personal information. Websites must also establish procedures that protect the confidentiality, security, and integrity of the personal information collected, including persistent identifiers used to recognize a user over time and across different websites, such as cookies.

Email Privacy Act:
In March 2013, a bipartisan coalition of Congressmen introduced the Email Privacy Act to reform ECPA. The bill would ensure electronic communications receive the same Fourth Amendment protections that snail mail and other paper documents receive.

Surveillance

Foreign Intelligence Surveillance Act (FISA) of 1978 and the FISA Amendments Act of 2008:
The FISA of 1978 created procedures for physical and electronic surveillance from foreign powers and agents of foreign powers, which may include American citizens and permanent residents suspected of espionage or terrorism. Congress passed an amendment to FISA in 2008 containing Section 702, which authorizes surveillance of people reasonably believed to be located outside the U.S., so long as they are not U.S. citizens or permanent residents.

Communications Assistance for Law Enforcement Act (CALEA):
CALEA was enacted in 1994 to enhance the ability of law enforcement agencies to conduct electronic surveillance. It requires that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities and services to have built-in surveillance capabilities.

USA Patriot Act:
The Patriot Act was passed in October 2001 in response to the September 11 terrorist attacks. It significantly increased the surveillance and investigative powers of law enforcement agencies. Discussion of specific provisions of the act can be found here.

USA Freedom Act:
The USA Freedom Act became law in June 2015, and ended the bulk collection of records about Americans under Section 215 and other provisions of the PATRIOT Act. Rather than bulk collection, specific selection terms are now required, and they must limit the scope of tangible things sought to the greatest extent possible. In addition, the Act permits companies to make additional reporting ranges to enhance transparency. The Act also requires the Foreign Intelligence Surveillance Court (FISC), which authorizes foreign intelligence surveillance requests, to publish significant opinions.

Additional Technology Issues

Telecommunications Act:
President Clinton signed this Act into law in 1996 and it was the first significant overhaul of U.S. telecommunications law since 1934. It required schools, libraries and hospitals to be connected to the Internet by 2000 and required the V-Chip to be installed into every new television, allowing parents to block certain television programs in their homes. The act also limited the number of radio or television stations one entity could own and allowed greater competition between telephone companies.

Computer Fraud and Abuse Act (CFAA):
CFAA is the federal anti-hacking law that makes it illegal to intentionally access a computer without authorization or to exceed authorized access. This is primarily a criminal law intended to reduce the instances of malicious hacking, but an amendment to the bill allows for civil actions to be brought under the statute. Some prosecutors have taken advantage of this confusion to bring criminal charges unrelated to hacking. For example, in cases such as *United States v. Drew* and *United States v. Nosal*, the government claimed that violating a private agreement or corporate policy amounts to a CFAA violation.

Digital Millennium Copyright Act (DMCA):
Passed in 1998, the Digital Millennium Copyright Act implements two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes technology, devices, or services intended to circumvent controlled access to copyrighted works. In addition, it heightens the penalties for copyright infringement on the Internet.