Chapter 2: Compliance - Laws and Ethics

Gonzalo De La Torre Parra, Ph.D.

Fall 2021

Google

- Google has fired Margaret Mitchell, co-lead of the ethical AI team, after she used an automated script to look through her emails in order to find evidence of discrimination against her coworker Timnit Gebru.

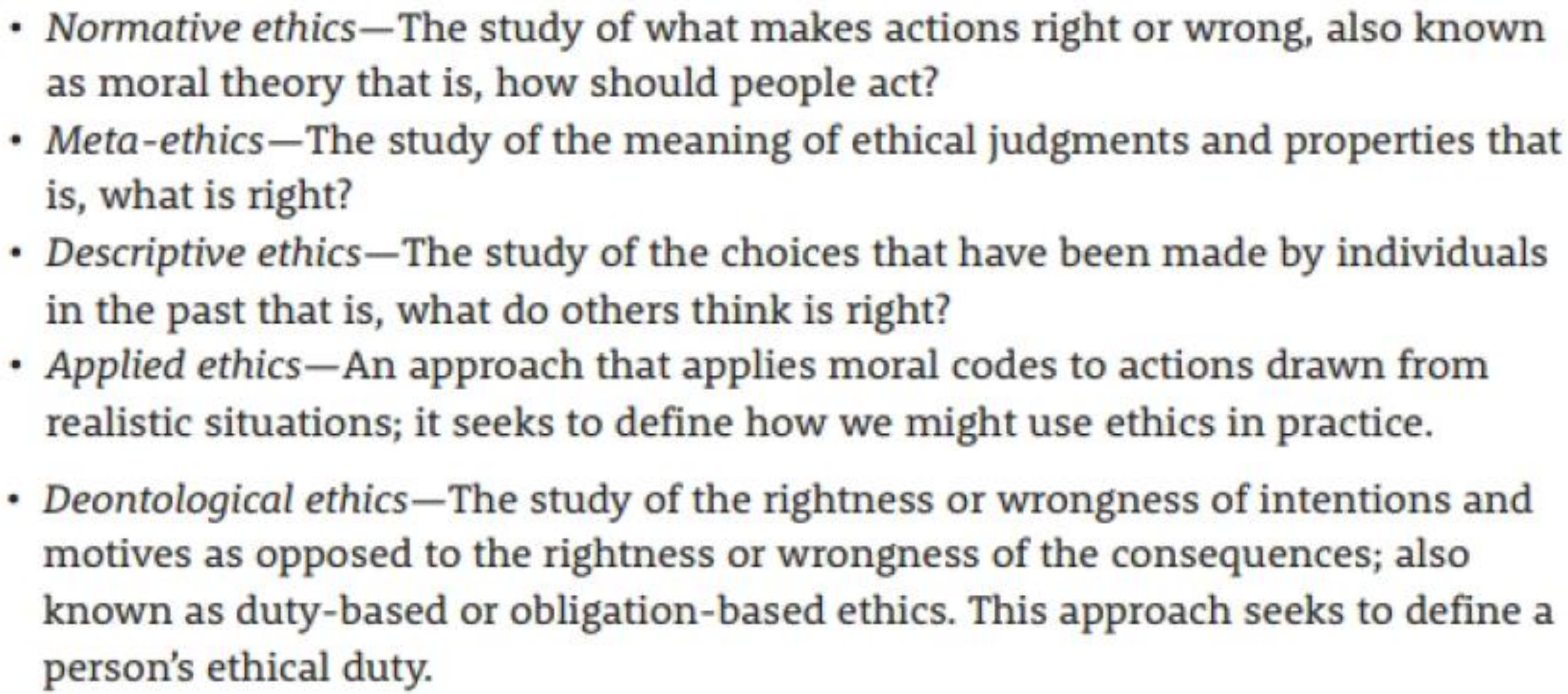
[Source: https://www.theverge.com/2021/2/19/22292011/google-second-ethical-ai-researcher-fired]

First event: “In his statement on Gebru’s departure last week claiming the paper was of poor quality, Google’s head of research, Jeff Dean, said it failed to cite research on making more efficient language models and ways to mitigate bias.”

[Source: https://www.wired.com/story/behind-paper-led-google-researchers-firing/]

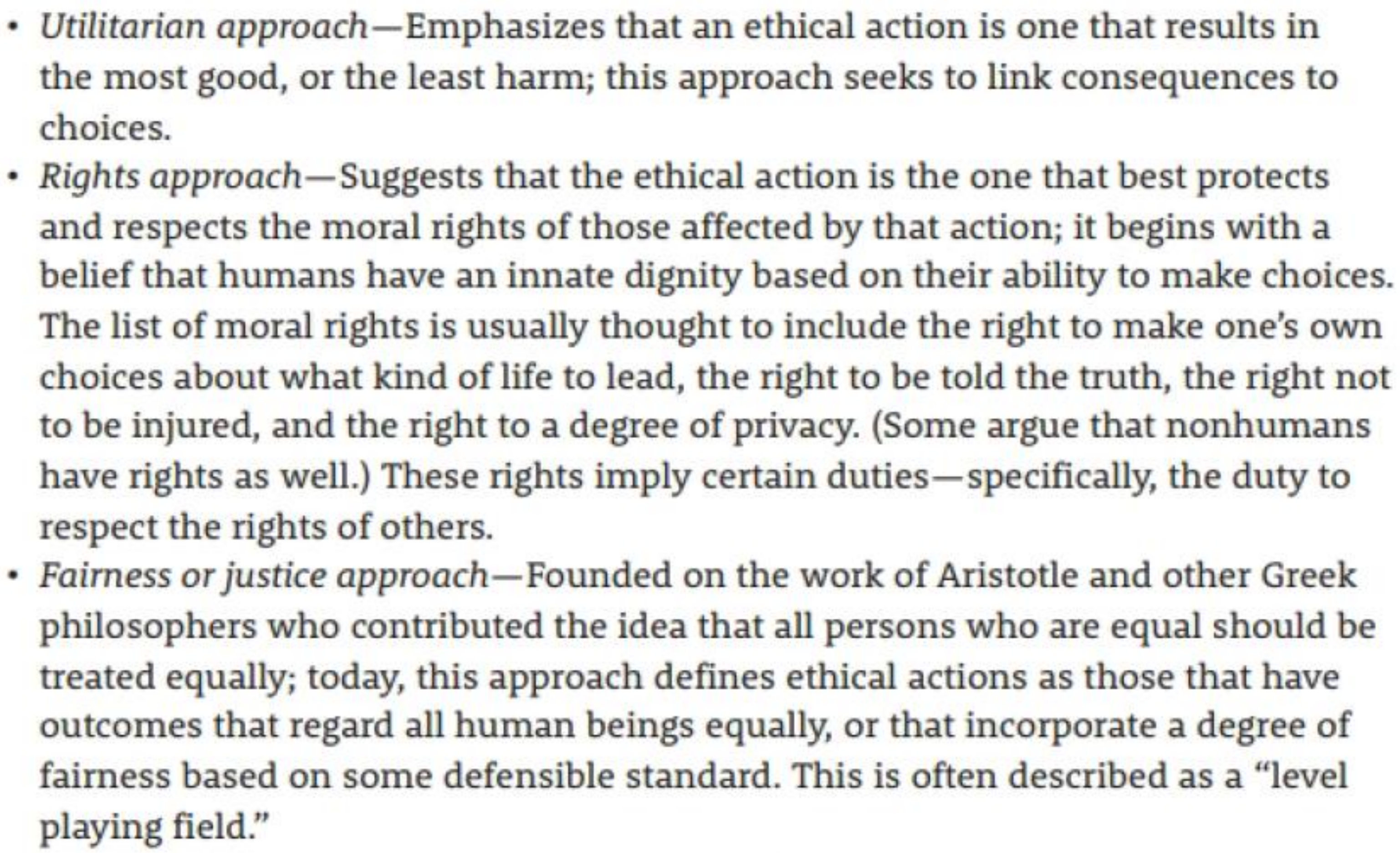
Ethics – Foundations and Frameworks

- The branch of philosophy that considers nature, criteria, sources, logic, and the validity of moral judgment.



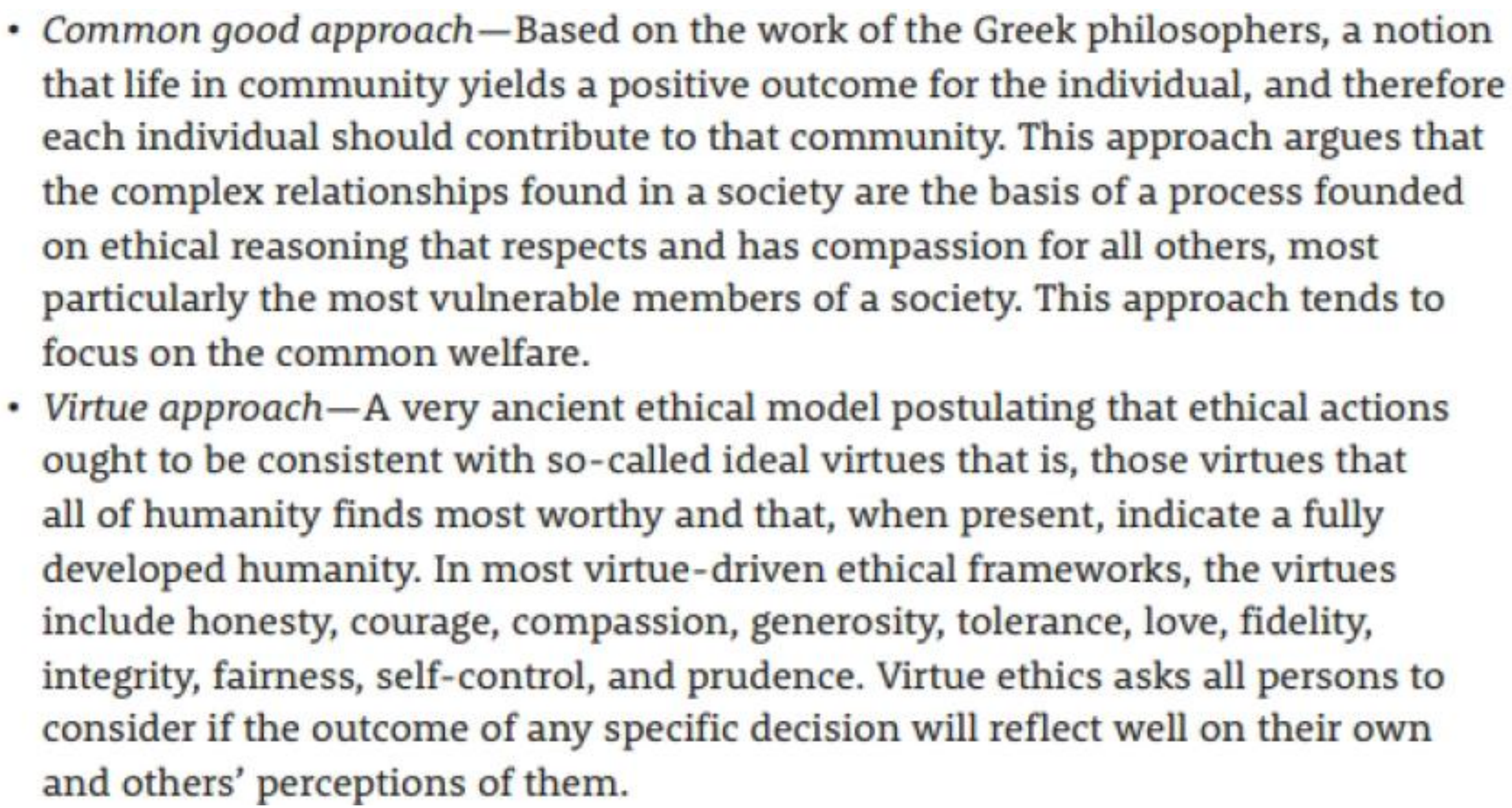
- *Normative ethics*—The study of what makes actions right or wrong, also known as moral theory that is, how should people act?
- *Meta-ethics*—The study of the meaning of ethical judgments and properties that is, what is right?
- *Descriptive ethics*—The study of the choices that have been made by individuals in the past that is, what do others think is right?
- *Applied ethics*—An approach that applies moral codes to actions drawn from realistic situations; it seeks to define how we might use ethics in practice.
- *Deontological ethics*—The study of the rightness or wrongness of intentions and motives as opposed to the rightness or wrongness of the consequences; also known as duty-based or obligation-based ethics. This approach seeks to define a person's ethical duty.

Ethical Standards



- *Utilitarian approach*—Emphasizes that an ethical action is one that results in the most good, or the least harm; this approach seeks to link consequences to choices.
- *Rights approach*—Suggests that the ethical action is the one that best protects and respects the moral rights of those affected by that action; it begins with a belief that humans have an innate dignity based on their ability to make choices. The list of moral rights is usually thought to include the right to make one's own choices about what kind of life to lead, the right to be told the truth, the right not to be injured, and the right to a degree of privacy. (Some argue that nonhumans have rights as well.) These rights imply certain duties—specifically, the duty to respect the rights of others.
- *Fairness or justice approach*—Founded on the work of Aristotle and other Greek philosophers who contributed the idea that all persons who are equal should be treated equally; today, this approach defines ethical actions as those that have outcomes that regard all human beings equally, or that incorporate a degree of fairness based on some defensible standard. This is often described as a "level playing field."

Ethical Standards



- *Common good approach*—Based on the work of the Greek philosophers, a notion that life in community yields a positive outcome for the individual, and therefore each individual should contribute to that community. This approach argues that the complex relationships found in a society are the basis of a process founded on ethical reasoning that respects and has compassion for all others, most particularly the most vulnerable members of a society. This approach tends to focus on the common welfare.
- *Virtue approach*—A very ancient ethical model postulating that ethical actions ought to be consistent with so-called ideal virtues that is, those virtues that all of humanity finds most worthy and that, when present, indicate a fully developed humanity. In most virtue-driven ethical frameworks, the virtues include honesty, courage, compassion, generosity, tolerance, love, fidelity, integrity, fairness, self-control, and prudence. Virtue ethics asks all persons to consider if the outcome of any specific decision will reflect well on their own and others' perceptions of them.

The Ten Commandments of Computer Ethics

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Deterring Unethical and Illegal Behavior

- It is the responsibility of InfoSec personnel to deter unethical and illegal acts, using policy, education and training, and technology as controls or safeguards, in order to protect the organization's information and systems.

General categories of unethical behavior that organizations and society should seek to eliminate

- Ignorance- As you learned earlier, ignorance of the law is no excuse, but ignorance of policies and procedures is.
- Accident- Individuals with authorization and privileges to manage information within the organization have the greatest opportunity to cause harm or damage by accident.
- Intent- Criminal or unethical intent refers to the state of mind of the individual committing the infraction. A legal defense can be built on whether the accused acted out of ignorance, by accident, or with the intent to cause harm or damage.

Deterrence

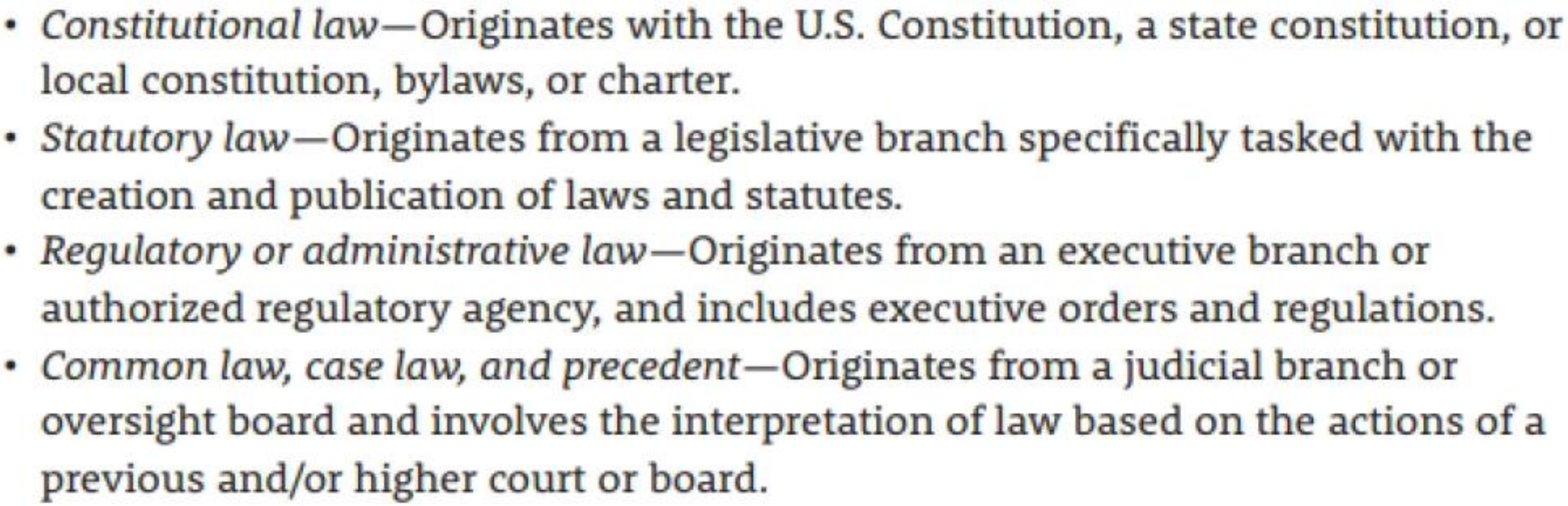
- Fear of penalty- Threats of informal reprimand or verbal warnings may not have the same impact as the threat of termination, imprisonment, or forfeiture of pay.
- Probability of being caught- There must be a strong possibility that perpetrators of illegal or unethical acts will be caught.
- Probability of penalty being administered- The organization must be willing and able to impose the penalty.

Professional Organizations and Their Codes of Conduct

- Association for Computing Machinery (ACM): The ACM's code of ethics requires members to perform their duties in a manner befitting an ethical computing professional.
- International Information Systems Security Certification Consortium, Inc. (ISC)2
- SANS
  - Respect for the Public
  - Respect for the Certification
  - Respect for My Employer
  - Respect for Myself

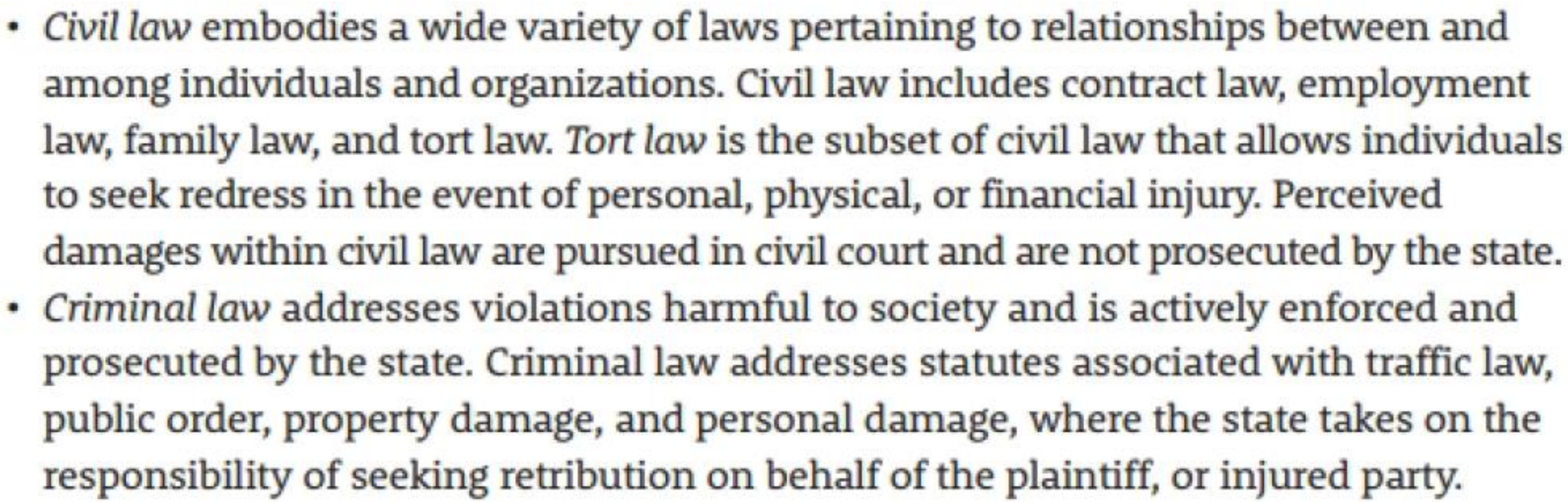
Information Security Laws

- Important to know legal framework within which their organizations operate.
- Types of Law:



  - *Constitutional law*—Originates with the U.S. Constitution, a state constitution, or local constitution, bylaws, or charter.
  - *Statutory law*—Originates from a legislative branch specifically tasked with the creation and publication of laws and statutes.
  - *Regulatory or administrative law*—Originates from an executive branch or authorized regulatory agency, and includes executive orders and regulations.
  - *Common law, case law, and precedent*—Originates from a judicial branch or oversight board and involves the interpretation of law based on the actions of a previous and/or higher court or board.

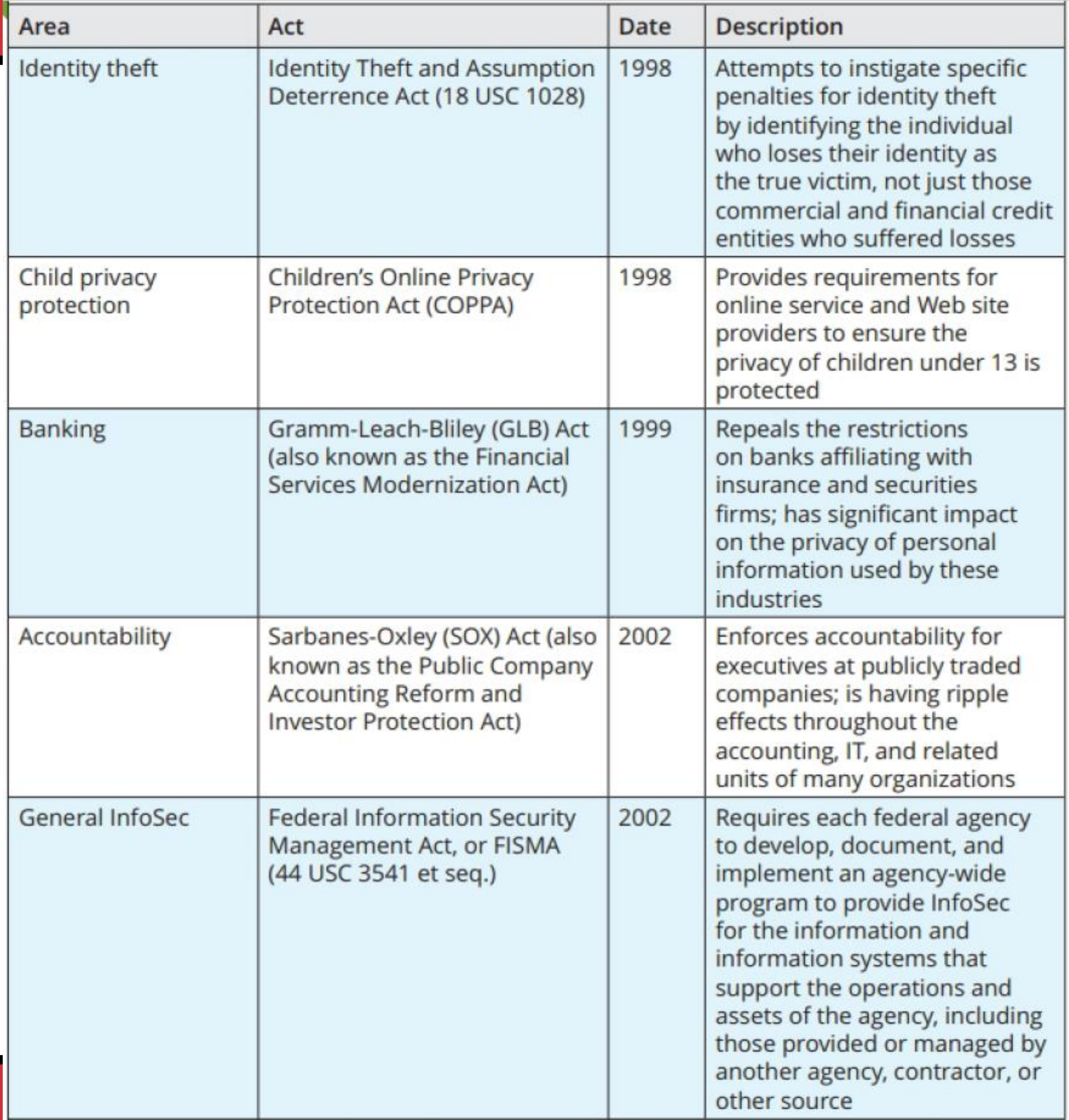
Statutory Law



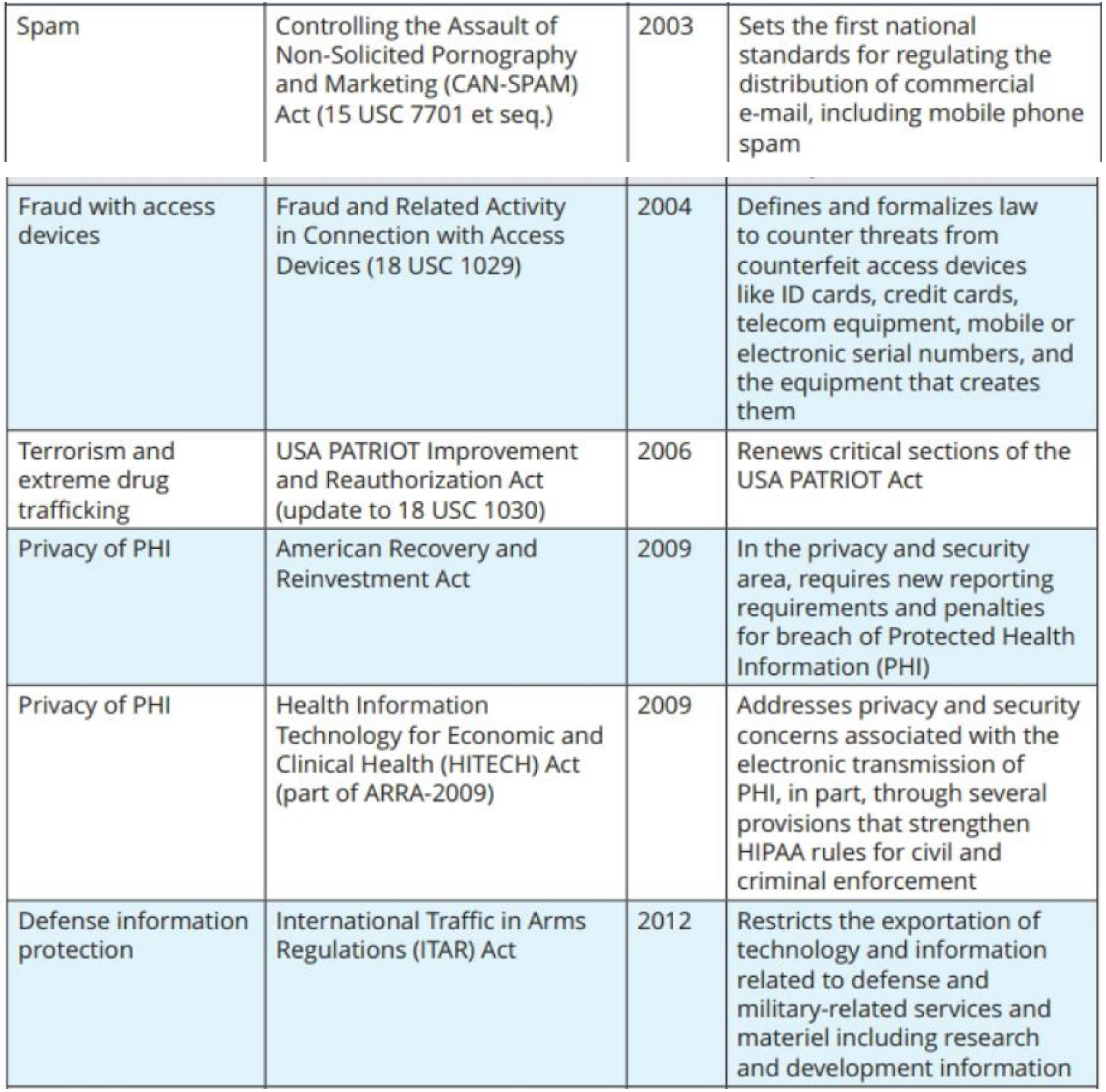
- *Civil law* embodies a wide variety of laws pertaining to relationships between and among individuals and organizations. Civil law includes contract law, employment law, family law, and tort law. *Tort law* is the subset of civil law that allows individuals to seek redress in the event of personal, physical, or financial injury. Perceived damages within civil law are pursued in civil court and are not prosecuted by the state.
- *Criminal law* addresses violations harmful to society and is actively enforced and prosecuted by the state. Criminal law addresses statutes associated with traffic law, public order, property damage, and personal damage, where the state takes on the responsibility of seeking retribution on behalf of the plaintiff, or injured party.

Relevant US Laws

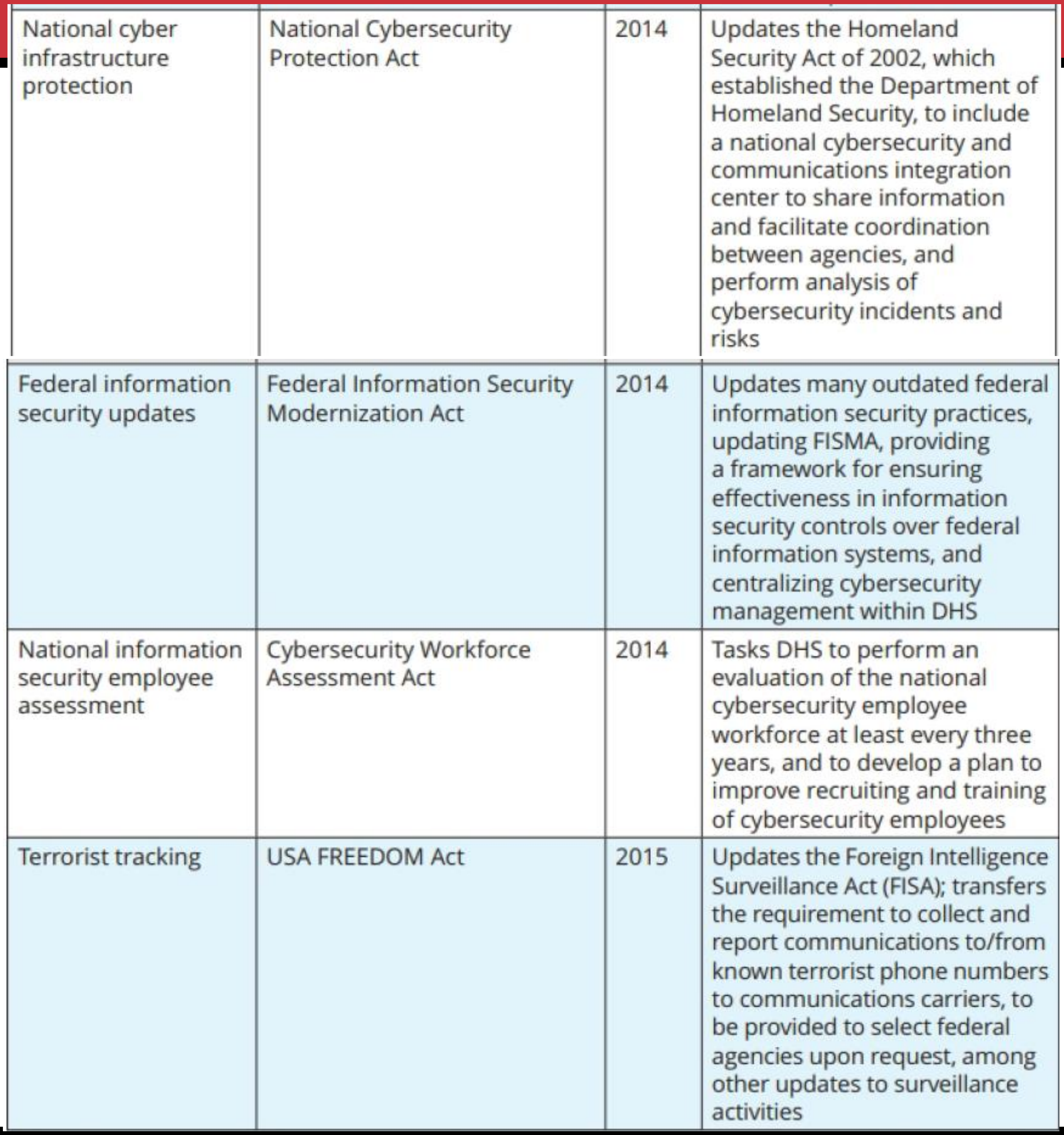
- Computer Fraud and Abuse (CFA) Act The cornerstone of many computer-related federal laws and enforcement efforts, the CFA formally criminalizes "accessing a computer without authorization or exceeding authorized access" for systems containing information of national interest as determined by the U.S. government.
- Computer Security Act (CSA) A U.S. law designed to improve security of federa l information systems. It charged the National Bureau of Standards, now NIST, with the development of standards, guidelines, and associated methods and techniques for computer systems, among other responsibilities.
- Electronic Communications Privacy Act (ECPA) of 1986 A collection of statutes that regulate the interception of wire, electronic, and oral communications. These statutes are frequently referred to as the "federal wiretapping acts."
- Health Insurance Portability and Accountability Act (HIPAA) of 1996 Also known as the Kennedy-Kassebaum Act, th is law attempts to protect the confidentiality and security of health care data by establishing and enforcing standards and by standardizing electronic data interchange.
- Privacy Act of 1974 A federal law that regulates the government's collection, storage, use, and dissemination of individual personal information contained in records maintained by the federal government.



Area	Act	Date	Description
Identity theft	Identity Theft and Assumption Deterrence Act (18 USC 1028)	1998	Attempts to instigate specific penalties for identity theft by identifying the individual who loses their identity as the true victim, not just those commercial and financial credit entities who suffered losses
Child privacy protection	Children's Online Privacy Protection Act (COPPA)	1998	Provides requirements for online service and Web site providers to ensure the privacy of children under 13 is protected
Banking	Gramm-Leach-Bliley (GLB) Act (also known as the Financial Services Modernization Act)	1999	Repeals the restrictions on banks affiliating with insurance and securities firms; has significant impact on the privacy of personal information used by these industries
Accountability	Sarbanes-Oxley (SOX) Act (also known as the Public Company Accounting Reform and Investor Protection Act)	2002	Enforces accountability for executives at publicly traded companies; is having ripple effects throughout the accounting, IT, and related units of many organizations
General InfoSec	Federal Information Security Management Act, or FISMA (44 USC 3541 et seq.)	2002	Requires each federal agency to develop, document, and implement an agency-wide program to provide InfoSec for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source



Spam	Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act (15 USC 7701 et seq.)	2003	Sets the first national standards for regulating the distribution of commercial e-mail, including mobile phone spam
Fraud with access devices	Fraud and Related Activity in Connection with Access Devices (18 USC 1029)	2004	Defines and formalizes law to counter threats from counterfeit access devices like ID cards, credit cards, telecom equipment, mobile or electronic serial numbers, and the equipment that creates them
Terrorism and extreme drug trafficking	USA PATRIOT Improvement and Reauthorization Act (update to 18 USC 1030)	2006	Renews critical sections of the USA PATRIOT Act
Privacy of PHI	American Recovery and Reinvestment Act	2009	In the privacy and security area, requires new reporting requirements and penalties for breach of Protected Health Information (PHI)
Privacy of PHI	Health Information Technology for Economic and Clinical Health (HITECH) Act (part of ARRA-2009)	2009	Addresses privacy and security concerns associated with the electronic transmission of PHI, in part, through several provisions that strengthen HIPAA rules for civil and criminal enforcement
Defense information protection	International Traffic in Arms Regulations (ITAR) Act	2012	Restricts the exportation of technology and information related to defense and military-related services and materiel including research and development information



National cyber infrastructure protection	National Cybersecurity Protection Act	2014	Updates the Homeland Security Act of 2002, which established the Department of Homeland Security, to include a national cybersecurity and communications integration center to share information and facilitate coordination between agencies, and perform analysis of cybersecurity incidents and risks
Federal information security updates	Federal Information Security Modernization Act	2014	Updates many outdated federal information security practices, updating FISMA, providing a framework for ensuring effectiveness in information security controls over federal information systems, and centralizing cybersecurity management within DHS
National information security employee assessment	Cybersecurity Workforce Assessment Act	2014	Tasks DHS to perform an evaluation of the national cybersecurity employee workforce at least every three years, and to develop a plan to improve recruiting and training of cybersecurity employees
Terrorist tracking	USA FREEDOM Act	2015	Updates the Foreign Intelligence Surveillance Act (FISA); transfers the requirement to collect and report communications to/from known terrorist phone numbers to communications carriers, to be provided to select federal agencies upon request, among other updates to surveillance activities

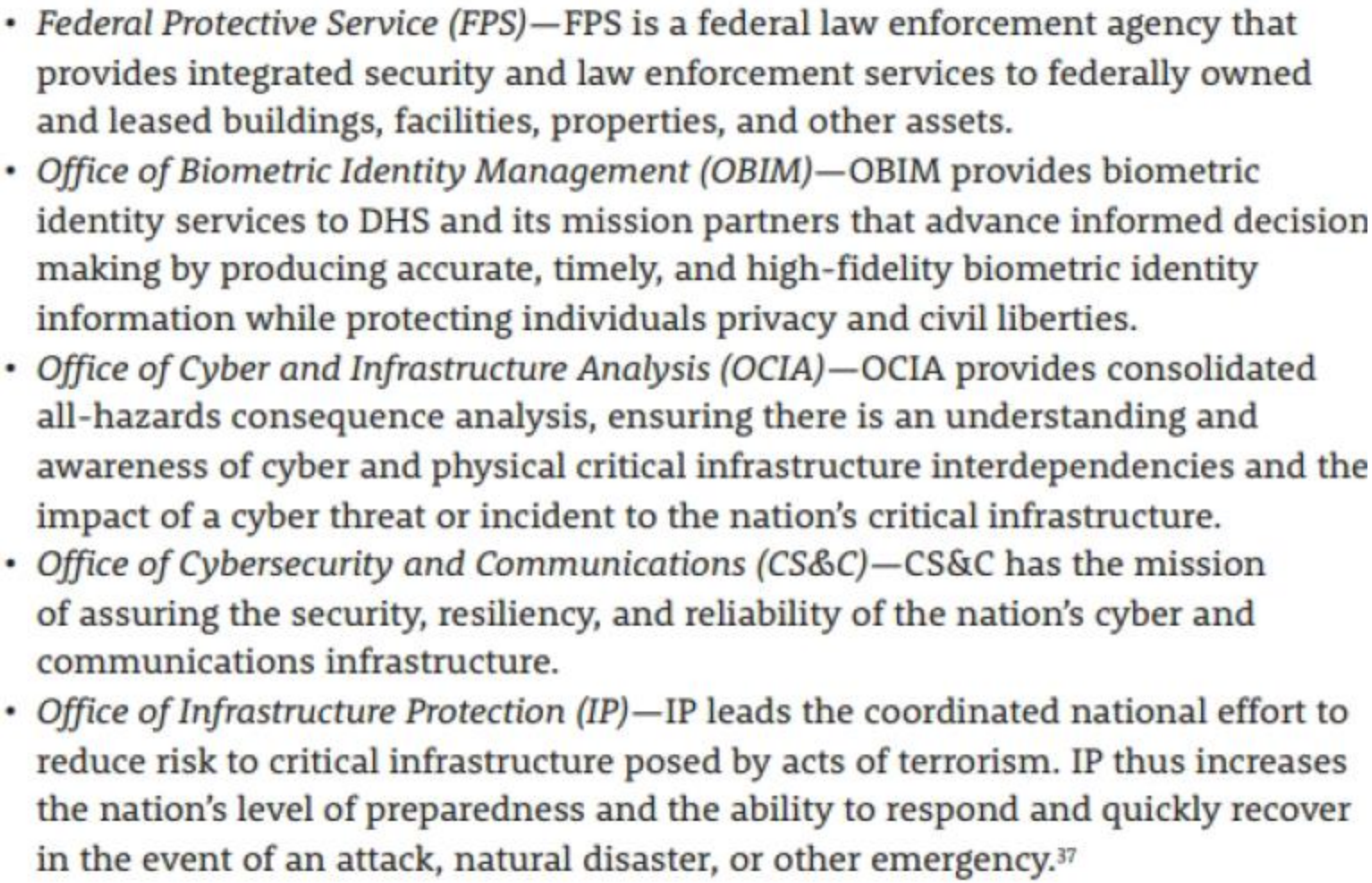
Patriot Act

- A mechanism to provide the United States with a means to investigate and respond to the 9/11 attacks on the New York World Trade Center. The USA PATRlOT Act provides law enforcement agencies with broader latitude to combat terrorism-related activities.
- Some of the laws modified by the USA PATRIOT Act are among the earliest laws created to deal with electronic technology. Certain portions of the USA PATRlOT Act were extended in 2006, 2010, and 2011.

Privacy Laws – HIPPA (Apr 14, 2013)

- The Health Insurance Portability and Accountability Act (HIPAA) of 1996, also known as the Kennedy-Kassebaum Act, attempts to protect the confidentiality and security of health care data by establishing and enforcing standards and by standardizing electronic data interchange.
- HIPAA affects all health care organizations, including small medical practices, health clinics, life insurers, and universities, as well as some organizations that have self-insured employee health programs.
- It provides for stiff penalties for organizations that fail to comply with the law, with up to $250,000 and/or 10 years imprisonment for knowingly misusing client information.
- The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule, located at 45 CPR Part 160 and Subparts A and C of Part 164, requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI."

Law Enforcement Agencies

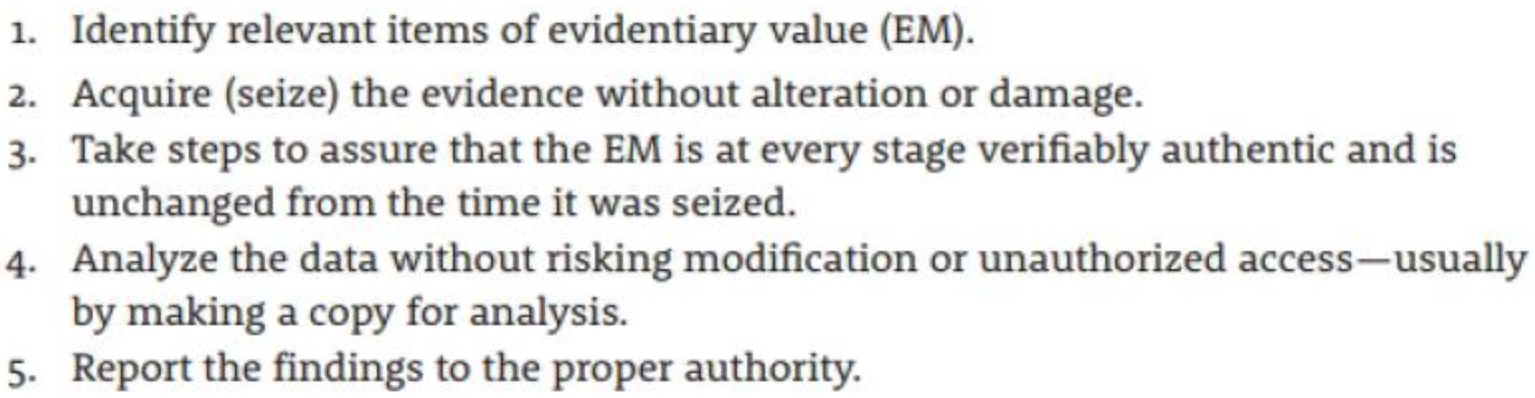


- *Federal Protective Service (FPS)*—FPS is a federal law enforcement agency that provides integrated security and law enforcement services to federally owned and leased buildings, facilities, properties, and other assets.
- *Office of Biometric Identity Management (OBIM)*—OBIM provides biometric identity services to DHS and its mission partners that advance informed decision making by producing accurate, timely, and high-fidelity biometric identity information while protecting individuals privacy and civil liberties.
- *Office of Cyber and Infrastructure Analysis (OCIA)*—OCIA provides consolidated all-hazards consequence analysis, ensuring there is an understanding and awareness of cyber and physical critical infrastructure interdependencies and the impact of a cyber threat or incident to the nation's critical infrastructure.
- *Office of Cybersecurity and Communications (CS&C)*—CS&C has the mission of assuring the security, resiliency, and reliability of the nation's cyber and communications infrastructure.
- *Office of Infrastructure Protection (IP)*—IP leads the coordinated national effort to reduce risk to critical infrastructure posed by acts of terrorism. IP thus increases the nation's level of preparedness and the ability to respond and quickly recover in the event of an attack, natural disaster, or other emergency.[37]

Digital Forensics

- Digital forensics involves applying traditional forensics methodologies to the digital arena, focusing on information stored in an electronic format on any one of a number of electronic devices that range from computers to mobile phones to portable media.
- Like forensics, it follows clear, well-defined methodologies but still tends to be as much art as science. This means the natural curiosity and personal skill of the investigator play a key role in discovering potential evidentiary material (EM), also known as items of potential evidentiary value.

Digital Forensics Methodology



1. Identify relevant items of evidentiary value (EM).
2. Acquire (seize) the evidence without alteration or damage.
3. Take steps to assure that the EM is at every stage verifiably authentic and is unchanged from the time it was seized.
4. Analyze the data without risking modification or unauthorized access—usually by making a copy for analysis.
5. Report the findings to the proper authority.

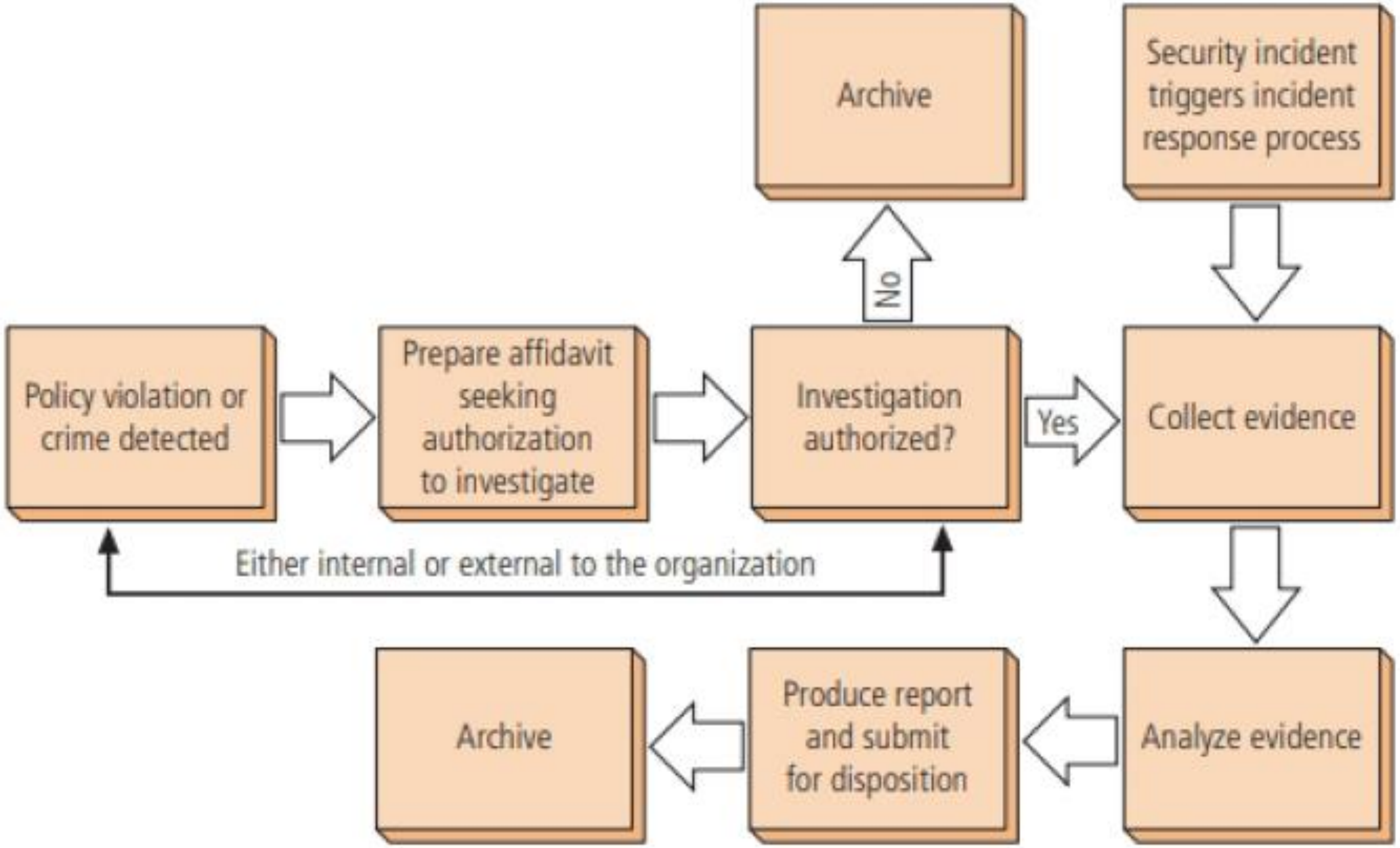
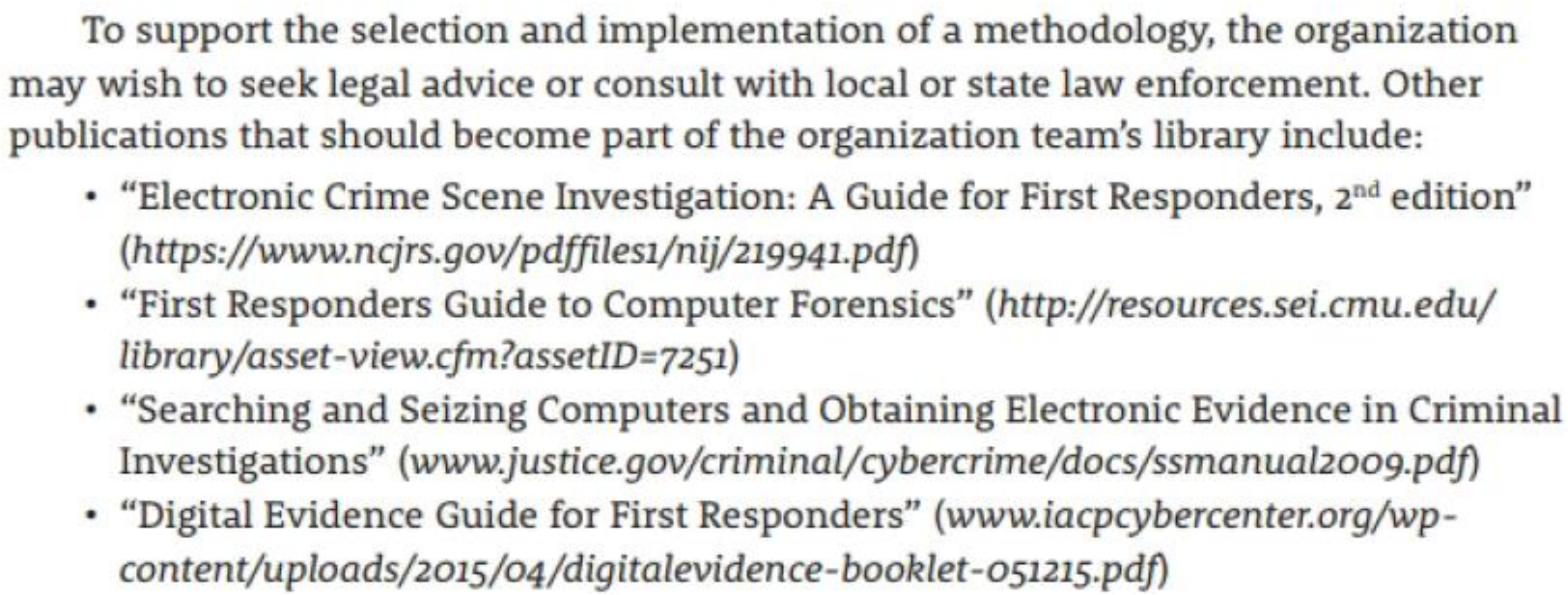

Archive
Security incident triggers incident response process
No
Policy violation or crime detected
Prepare affidavit seeking authorization to investigate
Investigation authorized?
Yes
Collect evidence
Either internal or external to the organization
Archive
Produce report and submit for disposition
Analyze evidence

Figure 2-2 Digital forensics process

Methodology Support



To support the selection and implementation of a methodology, the organization may wish to seek legal advice or consult with local or state law enforcement. Other publications that should become part of the organization team's library include:

- "Electronic Crime Scene Investigation: A Guide for First Responders, 2nd edition" (*https://www.ncjrs.gov/pdffiles1/nij/219941.pdf*)
- "First Responders Guide to Computer Forensics" (*http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=7251*)
- "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (*www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf*)
- "Digital Evidence Guide for First Responders" (*www.iacpcybercenter.org/wp-content/uploads/2015/04/digitalevidence-booklet-051215.pdf*)