The right to privacy became more specifically defined in a series of U.S. Supreme Court cases. In *Wheaten v. Peters* (1834), the court acknowledged that a person has an interest in being “let alone.” In 1890, Samuel Warren and Louis Brandeis explained this right to privacy in an article entitled, “The Right to Privacy.” They referred to it as “the right to be let alone.” Legal cases today still refer to this phrase.

The first U.S. Supreme Court decision to state that privacy was a constitutional right was *Griswold v. Connecticut* (1965). In this case, the Supreme Court found that the right to privacy was a fundamental right in the constitution.

In *Katz v. United States* (1967), Katz was making illegal bets using a public telephone. The government was using a listening device to tap the phone without a warrant. The Court found that the government violated Katz’s right to privacy even though he was using a public phone. In writing his concurring opinion, Justice Harlan coined the now-famous phrase, “a reasonable expectation of privacy.” The Court held that while the phone was a public pay phone, Katz had a reasonable expectation of privacy when using the phone.

Finally, in *Whalen v. Roe* (1977), the U.S. Supreme Court recognized a right to “informational privacy.” In this case, a New York law required doctors to report the names of patients who were prescribed narcotic drugs to the state using a state database. The Court upheld the law because it found that the law included procedures that properly protected the privacy of the information included in the database. The Court wrote, “We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files” (*Whalen v. Roe*).

There is not one comprehensive data privacy law in the United States; rather, there exists various different laws covering specific circumstances. The following are some of the laws that apply to data privacy:

**Census Confidentiality (1952)** – This law requires the U.S. Census Bureau to keep census responses confidential.

**Freedom of Information Act (1966)** – This Act establishes the public’s right to request information from federal agencies.

**Wiretap Act (1968)** – These statutes forbid the use of eavesdropping technologies without a court order. The law protects all email, radio communications, data transmission, and telephone calls.

**Mail Privacy Statute (1971)** – This law protects U.S. mail from being opened without the recipient’s consent.

**Privacy Act (1974)** – This Act applies to records created and used by federal agencies. It provides rules for the collection, use, and transfer of personally identifiable information, and requires federal agencies to have appropriate administrative, technical, and physical safeguards to protect the security of the systems and records they maintain.
Cable Communications Policy Act (1984) – This Act requires cable companies to inform customers about data collection and disclosure practices and requires them to ask permission to use the cable system to collect personal information.

Electronic Communications Privacy Act (1986) – This Act is an amendment to the Wiretap Act and includes additional communications like cell phones and texting.

Driver’s Privacy Protection Act (1994) – This Act requires states to protect the privacy of personal information contained in motor vehicle records. The passage of this law was motivated by the murder of a California actress by a stalker who obtained her home address from the California Department of Motor Vehicles.

E-Government Act (2002) – This Act requires the federal government to use information technologies that protect privacy and conduct Privacy Impact Assessments (PIAs). Additional industry-specific privacy laws covering financial data, medical data, government data, and children’s data will be discussed at length later in this course.

In addition to federal law, state law also addresses privacy. Ten state constitutions recognize a right to privacy. Other states recognize a right to privacy through case law. State governments have also created laws to protect data. Some 45 states and the District of Columbia have enacted breach notification laws that require an organization to notify state residents if it experiences a security breach that involves the personal information of the residents. Also, at least 29 states have laws requiring the proper disposal of paper and electronic information that contains personal data. Many states have passed industry specific laws that protect certain types of data like financial, health, and motor vehicle information. In 2013, legislation was pending in 36 states to prevent employers from asking employees for their social media passwords.

While the U.S. Supreme Court didn’t recognize constitutional privacy until 1965, U.S. common law has recognized privacy torts from as early as 1902. The common law is a body of law developed through court cases and legal tradition. U.S. common law was inherited from England. A tort is a civil action in which an injured party can sue a wrongdoer for damages. The common law of the United States recognizes the following privacy torts: intrusion into seclusion, portrayal in a false light, appropriation of a likeness or identity, and public disclosure of private affects. In deciding these cases, the court applies a “reasonable person” principle. In evaluating the case, the courts ask “How would an average person think or act?”

In 2009, the Ohio Supreme Court found that people have a reasonable expectation of privacy in their cell phones. In 1993, the Alabama Supreme Court heard a case involving the use of a photograph of a group of men at a dog track in the track’s advertising. The court dismissed the suit saying that there was nothing offensive about sitting at a dog track, and thus did not portray the men in a false light. In 1992, a court found that Samsung’s use of a robot in a blonde wig and an evening gown hosting a futuristic game show unlawfully appropriated the likeness of Vanna White. The Maryland Supreme Court held that the publishing of a plaintiff’s mug shot was not a public disclosure of private facts because the mug shot was originally part of the public record.

End