

Presentation to



Supporting digital freedom in Texas since 1990.

Illuminating the Penumbra: Deciphering the Constitutional Right to Information Privacy



Internet Communications Utilities Regulation

W. SCOTT MCCOLLOUGH
MCCOLLOUGH LAW FIRM PC

www.dotLAW.biz

2290 Gatlin Creek Rd.

Dripping Springs, Texas 78620

 512.888.1112

 512.692.2522

 wsmc@dotLAW.biz

September 10, 2018

Why is Privacy Important?

Privacy is important because it supports individual liberty and autonomy in liberal democratic societies. Privacy also has property implications. Finally, privacy provides functional benefits by advancing the human condition and preserving ordered, polite society.

What is “Privacy”?

“Private” and “privacy” derive from the Latin “*privus*” meaning “single” or “individual.”

Private is the opposite of public; privacy therefore involves something separate, or not involving “the public” (which can be “the people” or “the state”).

Judge Cooley, Warren and Brandeis called it “the right to be let alone.”

Pound and Freund characterized privacy as an extension of personality or personhood.

Prosser separated privacy litigation into four distinct but related legal torts: intrusion into solitude, publicizing private facts, false light and appropriation of name or likeness.

Moore describes privacy in terms of information control and supplies both normative and descriptive treatment. He argues that privacy is an information access and use control right.

Parent argues that “[p]rivacy is the condition of not having undocumented personal knowledge about one possessed by others.”

Inness defines privacy as “the state of possessing control over a realm of intimate decisions, which include decisions about intimate access, intimate information, and intimate actions.”

DeCew declares the “realm of the private to be whatever types of information and activities are not reasonably the legitimate concern of others.”

[Sourced from Moore, [Defining Privacy](#), 39 Journ. Social Philos. No. 3, 411-428 (2008)]

What is “Privacy”? (continued)

As a legal and philosophical matter, “privacy” derives from “liberty” and “property” concepts and, ultimately the ability to be an “individual” with a sense of and control over “the self.” These are the things the founders had in mind when they articulated the “unalienable” right to “life, liberty and the pursuit of happiness” in the Declaration of Independence.

Each of the express rights or liberties listed in the first eight amendments to the Constitution (speech and religion, bearing arms, freedom to not house soldiers, to be secure in their persons, houses papers and effects subject to warrant, no double jeopardy, no self-incrimination, no taking of life, liberty or property without due process and compensation, trial by jury, no excessive bail, fines or cruel and unusual punishment) create individual “zones of privacy” as against government. The Ninth Amendment does not mention liberty in particular, but it is important because it provides that there are additional rights (or liberties) retained by the people beyond those mentioned in the first eight amendments. The Tenth Amendment limits the federal government’s powers (including the judiciary) to only those expressly delegated by the Constitution. All other powers are “reserved” to the states “or to the people.” The due process clause of the Fourteenth Amendment then applies most (but not all) of the rights/liberties guaranteed in the first ten amendments to the states, including the right to privacy. The express rights/liberties expressly listed in the Constitution are not exhaustive; there are certain “unenumerated rights” as well and privacy is often said to be an “unenumerated right.”

Control over personal information about you (“Information privacy”) is one of several logically distinct kinds of “privacy” interests. These privacy interests flow from the right to speech ([*United States v. Rumely*](#)), to access information generated by others ([*Stanley v. Georgia*](#)), to associate with others ([*NAACP v. Patterson*](#)), and individual control over marital relations ([*Griswold v. Connecticut*](#)), contraception ([*Eisenstadt v. Baird*](#)) and abortion ([*Roe v. Wade*](#)).

The Court justified “finding” the right to abortion using both privacy and more general individual liberty rationalizations. *Roe* explains:

The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, going back perhaps as far as [1891], the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution...[P]ersonal rights that can be deemed “fundamental” or “implicit in the concept of ordered liberty,” are included in this guarantee of personal privacy. They also make it clear that the right has some extension to activities relating to marriage; procreation; contraception; family relationships; and child rearing and education.

410 U.S. at 152-153.

As a general matter, therefore, privacy in general and information privacy in particular come from the express rights in the first eight constitutional amendments and then more general notions of liberty and property. There are different kinds (although they sometimes overlap), and they are context-specific.

Philosophical Foundation: “Natural Law,” “Positive Law” and “Utilitarianism”

- “Natural Law” comes from philosophy. The doctrine asserts that individuals have certain inherent rights, endowed by nature—traditionally by God or a transcendent source—and that these can be understood universally through human reason. Natural law proponents often argue that humanity is best advanced through individual acts of self (and even selfish) determination, bounded by reason. Natural law is distinguished from “Positive Law”—human-made law that obliges action/inaction or describes the establishment of specific rights for an individual or group. Positive law comes from statutes, rules and binding case law.
- “Utilitarianism” is an ethical theory often used to advocate in favor of positive law. It holds that the best outcome is that which maximizes “utility” or the well-being of sentient entities, even to the detriment of an individual if necessary. Utilitarians are divided on whether actions/outcomes should be chosen based on their likely results (act utilitarianism) or whether agents should conform to rules that maximize utility (rule utilitarianism).
- Zones of privacy can be justified on both Natural Law and Utilitarian grounds. The natural law advocate will say it advances individual liberty, autonomy in decision-making, individual integrity and human dignity—all of which are said to be part of natural rights. The utilitarian will justify privacy norms on the ground they maximize utility by efficiently regulating social, family, professional and all other human relationships.

Natural Law Through the Ages

- Aristotle (384–322 BC) distinguished between the public and political sphere (the *polis*) and the private or domestic sphere of the family (the *oikos*). Each was distinct. The *Oikos* is a classical reference to a private “domain” outside the purview of government control. Aristotle believed that privacy was essential for individuals to pursue virtue by “turning away” from the masses; in his view “privacy” was not a right to do as one pleases, but instead an opportunity to do what one ought. According to Aristotle “The [wise man] is his own best friend, and takes delight in privacy whereas the man of no virtue or ability is his own worst enemy, and is afraid of solitude.”
- Saint Thomas Aquinas (1225–1274) attempted to synthesize Aristotelian philosophy and Catholicism, and is generally credited as the genesis of natural law theory. Like Aristotle, he advocated for individual reason in pursuit of virtue. He believed the natural order of justice limits rulers’ authority, and even rulers must obey the law: the state cannot exercise power over anyone unless the law permits it to do so through specific prescription. Power is justified only in service of the common good. Human rights have always existed with the human being, and human rights do not depend on the will of a state. A state cannot “create” human rights by law or by convention; government can only confirm their existence and give them protection. He also believed that intolerable tyranny had to be deposed through virtuous individual and collective action. Individuals are obliged to expose themselves to the peril of death for the liberation of the community.
- John Locke (1632–1704): “the State of Nature has a Law of Nature to govern it...and reason, which is that law, teaches all mankind...that being all equal and independent, *no one ought to harm another in his life, health, liberty, or possessions.*” (Second Treatise of Government). Locke articulated a broad view of “property” that includes a person’s rights, ideas, beliefs and the creative products of her labor with robust protection for the contents of expressive property including, but not limited to, private papers. *See, [Underkuffler, On Property: An Essay](#)* (“During the American Founding Era, property included not only external objects and people’s relationships to them, but also all of those human rights, liberties, powers, and immunities that are important for human well-being, including: freedom of expression, freedom of conscience, freedom from bodily harm, and free and equal opportunities to use personal faculties.”). To put it more simply and in somewhat circular fashion, our “rights” are our “property” under the Lockean view.
- John Stuart Mill (1806–1873) is sometimes classified as an “act utilitarian” and advocate of positive law, but he nonetheless implemented Aristotle’s spheres in [On Liberty](#) and used the public/private distinction to limit the appropriate realm of governmental authority and allow for a zone of “self-regulation” outside of government control. He addressed “self-regarding” and “other-regarding” individual action and argued that while the state could interfere and regulate “other regarding” action the “self-regarding” sphere is independent and the individual is sovereign.

The Founders Incorporated Natural Law Into the Constitution

- James Madison (1751-1836) often expressed Lockean views. He believed that a person's ideas, beliefs, abilities, and the opportunity to exercise them are the most treasured property. "A man has property in his opinions and the free communication of them," and "has a property of peculiar value in his religious opinions, and in the profession and practice dictated by them." The "safety and liberty of his person" is "property very dear to him." A "man is said to have a right to his property, he may be equally said to have a property in his rights." [Property, 6 the Writings of James Madison](#).
- Thomas Jefferson (1743-1826) [often explained](#) that the words he wrote in the Declaration of Independence regarding inalienable (natural) rights were incorporated into the Constitution, and a primary purpose of the Constitution was to secure and protect those rights. A few examples:

It is to secure our rights that we resort to government at all.

The principles on which we engaged, of which the charter of our independence is the record, were sanctioned by the laws of our being, and we but obeyed them in pursuing undeviatingly the course they called for. It issued finally in that inestimable state of freedom which alone can ensure to man the enjoyment of his equal rights.

Our legislators are not sufficiently apprised of the rightful limits of their power; that their true office is to declare and enforce only our natural rights and duties and to take none of them from us. No man has a natural right to commit aggression on the equal rights of another and this is all from which the laws ought to restrain him. * * * When the laws have declared and enforced all this, they have fulfilled their functions and the idea is quite unfounded that on entering into society we give up any natural right.

- John Adams (1735-1826) [expressed](#) similar sentiments:

"Rulers are no more than attorneys, agents, and trustees for the people" [and if rulers betray this trust] "the people have to revoke their authority" and substitute other agents, attorneys and trustees.

The Founders Incorporated Natural Law Into the Constitution (continued)

- Alexander Hamilton (1755-1804) discussed the principle as part of the debate leading up to the Declaration of Independence in a [letter](#) responding to the “Westchester Farmer’s” criticism of the legality of the Constitutional Congress:

... Apply yourself, without delay, to the study of the law of nature. I would recommend to your perusal, Grotius, Puffendorf, Locke, Montesquieu, and Burlamaqui. I might mention other excellent writers on this subject; but if you attend, diligently, to these, you will not require any others.

...

This is what is called the law of nature, “which, being coeval with mankind, and dictated by God himself, is, of course, superior in obligation to any other. It is binding over all the globe, in all countries, and at all times. No human laws are of any validity, if contrary to this; and such of them as are valid, derive all their authority, mediately, or immediately, from this original.” (Quoting Blackstone)

Upon this law, depend the natural rights of mankind, the supreme being gave existence to man, together with the means of preserving and beatifying that existence. He endowed him with rational faculties, by the help of which, to discern and pursue such things, as were consistent with his duty and interest, and invested him with an inviolable right to personal liberty, and personal safety.

Hence, in a state of nature, no man had any moral power to deprive another of his life, limbs, property or liberty; nor the least authority to command, or exact obedience from him; except that which arose from the ties of consanguinity.

Hence also, the origin of all civil government, justly established, must be a voluntary compact, between the rulers and the ruled; and must be liable to such limitations, as are necessary for the security of the absolute rights of the latter; for what original title can any man or set of men have, to govern others, except their own consent? To usurp dominion over a people, in their own despite, or to grasp at a more extensive power than they are willing to entrust, is to violate that law of nature, which gives every man a right to his personal liberty; and can, therefore, confer no obligation to obedience.

“The principal aim of society is to protect individuals, in the enjoyment of those absolute rights, which were vested in them by the immutable laws of nature; but which could not be preserved, in peace, without that mutual assistance, and intercourse, which is gained by the institution of friendly and social communities. Hence it follows, that the first and primary end of human laws, is to maintain and regulate these absolute rights of individuals.” (Quoting Blackstone)

- *See also* [Manion, Clarence Emmett, Founding Fathers and the Natural Law: A Study of the Source of our Legal Institutions \(1949\), Scholarly Works, Paper 1003](#) (providing additional historical citations and references)

The Courts and Natural Law

An individual's unalienable "Natural Law" right to privacy can supersede man-made "positive law."

- *Boyd v. United States* (1886) ("It is not the breaking of his doors and the rummaging of his drawers that constitutes the essence of the offence, but it is the invasion of his indefeasible right of personal security, personal liberty, and private property, where that right has never been forfeited by his conviction of some public offence.")
- *Berkowitz v. United States* (1st Cir. 1965) ("The American view of ordered liberty finds no clear distinction from totalitarianism or other forms of despotism than in our recognition that privacy is a principal object of civilization. We are held together as a community by our respect for one another.")
- *Mapp v. Ohio* (1961) ("Every person has the 'liberty' of being free from unwarranted government intrusion into the individual's private affairs. We find that ... the freedom from unconscionable invasions of privacy ... enjoy an 'intimate relation' in their perpetuation of principles of humanity and civil liberty [secured] . . . only after years of struggle. They express 'supplementing phases of the same constitutional purpose to maintain inviolate large areas of personal privacy.'")

Roman Law Recognized the Right to Privacy

The punishment of one who had not committed any assault upon another or impeded in any way his right of locomotion, but who merely attracted public attention to the other as he was passing along a public highway or standing upon his private grounds, evidences the fact that the ancient law recognized that a person had a legal right 'to be let alone,' so long as he was not interfering with the rights of other individuals or of the public. Sandar's Just. (Hammond's ed.) 499; Poste's Inst. Gaius (3d ed.), 449. Under the Roman law, 'to enter a man's house against his will, even to serve a summons, was regarded as an invasion of his privacy.' Hunter's Roman Law (3d ed.), 149. 4 Bl. 168.

[*Pavesich v. New England Life Ins. Co.*](#) (Ga. 1905)

Pavesich at 71 draws a direct line from Roman law to British common law:

In Semayne's case (5 Coke, 91), 1 Smith's Lead. Cas. 228, where this maxim was applied, one of the points resolved was 'That the house of every one is to him as his castle and fortress, as well for his defence against injury and violence as for his repose.' 'Eavesdroppers, or such as listen under walls or windows or the eaves of a house to hearken after discourse, and thereupon to frame slanderous and mischievous tales,' were a nuisance at common law and indictable, and were required, in the discretion of the court, to find sureties for their good behavior. 4 Bl. 168. The offense consists in lingering about dwelling-houses and other places where persons meet for private intercourse and listening to what is said, and then tattling it abroad. 10 Am. & Eng. Enc. L (2d ed.) 440. A common scold was at common law indictable as a public nuisance to her neighborhood. 4 Bl. 168. And the reason for the punishment of such a character was not the protection of any property right of her neighbors, but the fact that her conduct was a disturbance of their right to quiet and repose, the offense being complete even when the party indicted committed it upon her own premises. Instances might be multiplied where the common law has both tacitly and expressly recognized the right of an individual to repose and privacy.

British Common Law Expanded the Roman Right to Privacy

- [*Entick v Carrington*](#), 19 How. St. Tr. 1029, 1066 (1765):

Papers are the owner’s goods and chattels[.] [T]hey are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect. Where is the written law that gives any magistrate such a power? I can safely answer, there is none; and therefore it is too much for us without such authority to pronounce a practice legal, which would be subversive of all the comforts of society.
- [*Millar v. Taylor*](#), 4 Burr. 2303, 2379 (1769):

It is certain every man has a right to keep his own sentiments, if he pleases. He has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends.
- Privacy-related considerations also protected against nonconsensual publication of writings, drawings or property inventories, in England and the United States. [*Prince Albert v. Strange*](#), 2 DeGex & Sm. 652, 696, 697 (1849), on appeal, 1 McN. & G. 25 (1849) (London); [*Kiernan v. Manhattan Quotation Co.*](#), 50 How. Pr. 194 (1876) (New York).
- Publication of private information could be enjoined even if it had been conveyed to a third party, who then committed a “breach of trust” by trying to reveal the information. [*Yovatt v. Winyard*](#), 37 Eng. Rep. 425 (Ch. 1820); [*Morison v. Moat*](#), 9 Hare, 241, 255 (1851). This precedent undermines the Supreme Court’s dogged adherence to the so-called “Third Party Doctrine” as an exception to the “reasonable expectation of privacy” test often used for Fourth Amendment purposes.

Efforts to Protect Information Privacy Through History

- “Cryptology” is Greek for “hidden words.”
- The goal is to keep a communication secret from all but the intended recipient.
- There are three general types: Ciphers, Codes and Concealments.
 - **Ciphering** involves treatment of textual units of constant and equal length, usually single letters although two or three are sometimes used. The textual units are each treated as symbols without reference to any identity as a component part of a word, phrase or sentence. A key is used to encode or decode. Ciphers typically employ “transposition” (rearrangement without change in identity) or “substitution” (replace letter symbol with some other symbol).
 - **Code** is a type of substitution, except unlike cipher substitution the treatment applies varying and unequal lengths.
 - **Concealment** (Steganography) hides the text within an external or apparently innocent writing or item, and disguises that there is even a message. Disappearing ink and microdots are good examples.

Efforts to Protect Information Privacy Through History (continued)

- Early Chinese leveraged the ideographic nature of their language to hide meaning of words, a form of concealment.
- In India early rulers used alphabetic substitution codes through phonetics, and often communicated the message using sign language. The [Kama Sutra](#) has a section on how to cypher.
- The [Sumerians](#) and Ancient Egyptians used cryptography in 3500 BC and sometimes compounded by substituting between cuneiform and hieroglyphs.
- Mesopotamians, Babylonians and Assyrians used cuneiforms to encipher during the same period.
- Hebrews did substitution ciphers using Roman alphabet in 600 BC.
- The Spartans used transposition ciphering in 500 BC by wrapping leather or parchment around a cylinder or other object (scytale), writing the message and then unwrapping.
- In 499 BC Histiaeus employed concealment by shaving the head of a slave and then tattooing a message telling Aristagoras to revolt against the Persians. But he had to wait until the slave's hair grew back.
- Ciphering and code considerably advanced in the 15th and 16th centuries, with several methods devised to both encrypt and break codes.
- Mary, Queen of Scots tried to use a cipher while conspiring against Queen Elizabeth I. Elizabeth's chief code breaker did his job, and Mary was executed in 1587.
- The British and American revolutionaries used ciphers, codes and invisible ink during the Revolutionary War.
- Thomas Jefferson [used codes](#) (and even invented a Wheel Cipher although he apparently never used it) during his ambassadorship to France (from 1784 to 1789) because European postmasters routinely opened and read all diplomatic and any suspect letters passing through their command.
- Jefferson's Wheel Cipher was "reinvented" in 1917 and called the "M-94/CSP 488." The military [used this cipher between 1922 and 1945](#), until it was replaced by electromechanical rotor machines like the [M-209](#).
- The most famous cipher is the [Enigma machine](#) (also an electromechanical rotor machine) devised by the Germans in WWII, but it was ultimately broken. Few realize that the most effective code (never broken) was the use of Native American and Basque "Code Talkers" in both world wars, who combined obscure languages and dialects with strategic word substitution ("turtle"="tank"; "sewing machine"="machine gun").
- Today, most encryption is done electronically, with block cipher becoming predominant, although there is still some stream ciphering (bit-by-bit).

Means to Protect Information Privacy/Security

- Fourth Amendment: Requires a warrant based on probable cause before a “search” or “seizure” can occur. This amendment is discussed further below.
- Fifth Amendment: The Fifth Amendment prohibits authorities from compelling a person to be “a witness against himself.” It is the “right to remain silent” and relates to testimonial evidence—statements spoken by the person while under oath. It also protects against the production of certain documents under the so-called “Act of Production Doctrine.” Producing documents or materials (*e.g.*, in response to a subpoena) may have a “testimonial aspect” for purposes of the individual’s right to assert the Fifth Amendment right against self-incrimination to the extent that the individual’s act of production provides information not already in the hands of law enforcement personnel about the existence, custody or authenticity, of the documents or materials produced. [*United States v. Hubbell*](#).
- [*Boyd v. United States*](#) held that the Fifth Amendment also protects against compulsory production of potentially incriminating private books and papers (even in the civil context, if fines or forfeitures are involved) pursuant to a subpoena, even though the same materials may properly be the subject of a valid Fourth Amendment warrant. The Supreme Court recently made clear that the right [must be expressly invoked](#) and prosecutors can comment on the fact that it was invoked.
- The caselaw on whether a person can be compelled to reveal an encryption key or produce an unencrypted copy is mixed and confusing. One can roughly analogize to physical locks. If there is a physical key production can often be compelled because the Fifth Amendment does not prevent compelled physical acts. If the lock requires a combination, then the person must “use his mind” and cannot be compelled to disclose the combination. But he or she might still be required to come and open the lock under the “foregone conclusion” doctrine. Most scholars and courts conclude that the government can probably require a suspect to unlock encryption that uses biometric keys like fingerprints or face recognition because those do not involve use of the mind. Law enforcement can compel production of a plaintext document that contains all passwords and keys the person uses. If a third party knows the key they can be compelled to disclose it. **The safest course is to use a key that only you control, and is retained solely in your brain. Do not tell anyone what the key is, never disclose that the files exist and don’t tell anyone what they contain.**
 - The touchstone of whether an act of production is testimonial is whether the government compels the individual to use “the contents of his own mind” to explicitly or implicitly communicate some statement of fact. [*Curcio v. United States*](#) (1957).
 - [*In re Boucher*](#) (2009), the US District Court of Vermont ruled that the Fifth Amendment might protect a defendant from having to reveal an encryption password, or even the existence of one, if the production of that password could be deemed a self-incriminating “act” under the Fifth Amendment. In *Boucher*, production of the unencrypted drive was deemed not to be a self-incriminating act, as the government already had sufficient evidence to tie the encrypted data to the defendant. Compelled disclosure of the key was allowed under the “foregone conclusions doctrine” (compelled reveal of something the government already knows is not testimonial).

Means to Protect Information Privacy/Security (continued)

- In January 2012 a federal judge in Colorado [ruled](#) that a suspect was required to give an unencrypted copy of a laptop hard drive to prosecutors based on the foregone conclusion doctrine. The Eleventh Circuit, however, [reversed](#) an order requiring a defendant to produce a decrypted copies of digital files thought to contain child pornography in response to a grand jury subpoena. Production required a testimonial act since doing so conceded existence, possession, control and authenticity.
- [This April 2018 article](#) by Orin Kerr discusses two relatively recent decisions. Kerr is an acknowledged authority in this field, but his conclusions tend to be less protective of individual rights and more deferential to law enforcement, so we part ways from time to time. The Supreme Court rejected his analysis of whether historical cell site information was protected under the Fourth Amendment based on the “Third Party Doctrine” in [Carpenter v. United States](#), as Justice Gorsuch notes in his dissent.

Means to Protect Information Privacy/Security (continued)

- A very recent state court case from Indiana (*Seo v. Indiana*, 2018 Ind. App. LEXIS 290 (Aug. 22, 2018)) accepts a new argument in favor of Fifth Amendment protection. The state appeals court found that forced decryption requires the defendant to “recreate the information the state is seeking” and this is “testimonial”:

[W]e consider [Kaitlin] Seo’s act of unlocking, and therefore decrypting the contents of her phone, to be testimonial not simply because the passcode is akin to the combination to a wall safe as discussed in *Doe*. We also consider it testimonial because her act of unlocking, and thereby decrypting, her phone effectively recreates the files sought by the State. As discussed above, when the contents of a phone, or any other storage device, are encrypted, the cyphertext is unintelligible, indistinguishable from random noise. In a very real sense, the files do not exist on the phone in any meaningful way until the passcode is entered and the files sought are decrypted. Thus, compelling Seo to unlock her phone goes far beyond the mere production of paper documents at issue in *Fisher*, *Doe*, or *Hubbell*. **Because compelling Seo to unlock her phone compels her to literally recreate the information the State is seeking, we consider this recreation of digital information to be more testimonial in nature than the mere production of paper documents.** (emphasis added)

The *Seo* court also rejected the government’s argument that unlocking a phone for police is different and less problematic under the Fifth Amendment than turning over a password to police:

[B]ecause we believe that electronic data and the devices that contain it are fundamentally different than paper documents and paper storage, we reject the State’s attempt to distinguish between compelling Seo to convey her passcode to the State and compelling Seo to simply unlock her phone by entering the passcode itself. **It is a distinction without a difference because the end result is the same: the State is compelling Seo to divulge the contents of her mind to obtain incriminating evidence.** (emphasis added)

This analysis seems correct from a technical perspective. The theory that forced encryption requires recreation and is therefore testimonial is separate from different from whether revealing or entering a password is testimonial, however, has not been addressed by any federal court. Stay tuned for future developments.

Means to Protect Information Privacy/Security (continued)

- Testimonial/production privileges: some relationships like marriage, doctor/patient, priest/penitent and lawyer/client allow a person to prevent the other person in the relationship from testifying about any “privileged” material. Time has gradually eroded many of these privileges, especially with regard to documents, through various court-crafted exceptions. Legislatures can sometimes overrule the privilege as well, and they have in areas like child abuse. A person in a protected relationship can therefore sometimes be obliged to report and disclose incriminating statements by the other person notwithstanding the privilege.
- Civil actions: the courts have long recognized certain actions at law or in equity to prevent or stop the public disclosure of private or protected facts. Some sound in tort, some arise from property rights, some come from the law of contracts and others (like copyright) are the result of legislation.
- **If you really want to keep a secret you control, don’t write it and don’t share any hint of it. There is no absolute certainty once you do either of these things.**

“Information Privacy” As a Discrete Privacy Right

Information privacy as a specific unenumerated right has experienced twists and turns, even in the Fourth Amendment context where protections are usually the greatest. Information held (stored) in the home receives the most protection. Things get complicated when the information exists outside the home, especially if it is handled or in the hands of third parties.

- Digital information in the home is the same as information on paper. Covered by the Fourth Amendment and accessible to law enforcement only pursuant to a warrant supported by probable cause.
- Digital information on a cell phone is now protected by the Fourth Amendment, even in the context of a custodial search incident to arrest. [*Riley v. California*](#).
- The Supreme Court has not addressed the broader issue of digital information on a laptop or portable storage media, but one would expect a similar outcome to that in *Riley*. There is an exception for searches close to border areas or in ports of entry for routine searches that are not prolonged or intrusive. Under [*United States v. Cotterman*](#) (Ninth Circuit, 2013) prolonged or intrusive border searches require some basis for suspicion of criminal activity (a standard lower than probable cause). [*United States v. Kim*](#) (D.C.D.C. 2015) applied a probable cause standard to border searches and refused to apply a custodial search exception, in part by relying on *Riley*.
- Long term surveillance via a GPS device surreptitiously placed on a vehicle violates the Fourth Amendment. [*United States v. Jones*](#).
- There is a “Third Party Doctrine” exception in the Fourth Amendment jurisprudence. [*United States v. Miller*](#) (bank records); [*Smith v. Maryland*](#) (dialed numbers). The basic notion is that you have no property right and no reasonable expectation of privacy to private or revealing information held or generated by a third party. Thus the information can be obtained from that third party with a mere subpoena. Many commentators (including your humble presenter) have strongly criticized the Third Party Doctrine’s basis, conceptualization and the obviously subjective (mis)application over the years. The theoretical foundation is faulty, since there are several forms of action in law and equity to prevent a third party from revealing private information, and one often *does* have a property interest. The better approach is to use “bailment” theory for this type information.
- The Supreme Court decided [*Carpenter v. United States*](#) in June. The Court refused to “extend” the third party doctrine to historical cell site information generated by cell companies, but did not repudiate the doctrine. Justice Gorsuch dissented, but he would have reached the same result using several different theories, including the notion that digital information can be property for Fourth Amendment purposes and when held by third parties bailment principles may well apply. Third parties that hold this information about you are (or should be) mere bailees that have a duty to preserve and protect this information by insisting on a probable cause warrant with sufficient particularity before they turn it over.

Is Information Privacy Threatened by Supreme Court Membership Turnover?

There is some legitimate concern over potential future developments as the Supreme Court's composition changes, including in the privacy and liberty area. This is especially so with regard to abortion. As noted, information privacy and abortion both ultimately relate to the liberty-based "right of self-determination" and to be "let alone." Since a woman's body is her own property there are property interests too. But abortion and information privacy involve different considerations and different activity. Regardless of its perceived merits or demerits based on one's political, ethical or moral bent, the "privacy" basis for abortion is qualitatively different from information privacy as a matter of ethics and law.

One main difference is that a woman's right to choose whether to abort a nonviable fetus has some limits and may be subjected to reasonable regulation, largely because the Court has found there are legitimate countervailing interests. The state may ensure medical procedures are performed safely, at least insofar as any regulations do not place a "substantial obstacle in the path of a woman's choice." [*Planned Parenthood v. Casey*](#); [*Whole Woman's Health v. Hellerstedt*](#). The State also "has an important and legitimate interest in protecting the potentiality of human life. These [two state] interests are separate and distinct. Each grows in substantiality as the woman approaches term and, at a point during pregnancy, each becomes 'compelling'." [*Roe v. Wade*](#). Abortion pertains to a "unique" form of permitted action by an *individual* that also impacts others.¹

Digital privacy, however, concerns intensely private *information* about the individual and the issue is the extent to which *government* may coercively obtain that information and use it for purposes antagonistic to the individual's interest. Information privacy is not subject to the kind of countervailing interests that exist with regard to abortion, and no case has held that what you do with your private information is subject to "reasonable regulation."²

¹ Abortion is a unique act. It is an act fraught with consequences for others: for the woman who must live with the implications of her decision; for the persons who perform and assist in the procedure; for the spouse, family, and society which must confront the knowledge that these procedures exist, procedures some deem nothing short of an act of violence against innocent human life; and, depending on one's beliefs, for the life or potential life that is aborted. Though abortion is conduct, it does not follow that the State is entitled to proscribe it in all instances. That is because the liberty of the woman is at stake in a sense unique to the human condition and so unique to the law.

[*Planned Parenthood v. Casey*](#), 505 U.S. at 852 (emphasis added).

² There is "regulation" concerning what *others* do with information they hold about you. Notable examples are telecommunications, cable service, health and banking. There are also record-keeping, retention and production regulations for certain businesses, including those run as sole proprietorships. But no regulation applies to individuals on matters related to their private lives other than those promulgated by tax authorities.

Is Information Privacy Threatened by Supreme Court Membership Turnover? (continued)

Some have questioned whether the two most recent Trump appointees may lead a revolt against the current decisional trend in favor of information privacy.

Justice Gorsuch's *Carpenter* dissent should quell some of that concern. Brett Kavanaugh's appointment has revived the issue, given his concurring opinion in [*Klayman v. Obama*](#), 805 F.3d 1148, 1148-1149 (D.C. Cir. 2015). Judge Kavanaugh concurred in a *per curiam* denial of emergency rehearing *en banc* of a panel decision approving the government's later-replaced "metadata collection program" operated for "national security" purposes in the face of a Fourth Amendment challenge. The relatively short concurrence had two parts. First, Judge Kavanaugh followed the then-prevailing Supreme Court "Third Party Doctrine" precedent by holding the information was "non-content" and generated and then retained by service providers. It was therefore not obtained through a "search" under the then-prevailing precedent. Second, he held that even if it was a search individual privacy interests were outweighed by the government's "'special need' — that is, a need beyond the normal need for law enforcement — that outweighs the intrusion on individual liberty." Specifically, he asserted that "bulk collection of telephony metadata serves a critically important special need — preventing terrorist attacks on the United States." 805 F.3d at 1149.

Carpenter – decided after *Klayman* and shortly before Kavanaugh's nomination – materially changed the Third Party Doctrine. Governmental acquisition of similar non-content information from "third party" providers is now a "search" and requires a warrant. The *Carpenter* majority cautioned against rote application of the ruling to "other collection techniques involving foreign affairs or national security," 2011 L. Ed. at 525, but one would be hard pressed to argue that the metadata program was less revealing and less intrusive than the CSLI addressed in *Carpenter*. One would expect Judge Kavanaugh to recognize the change in law and hold that metadata acquisition is now a search. He would then have to confront the question of whether the search is sufficiently "reasonable" to dispense with the warrant requirement. As in *Klayman* the specific question would be whether any asserted national security needs are "special" and sufficiently "beyond the normal need for law enforcement" to justify the "intrusion on individual liberty." 805 F.3d at 1149. "Justice" Kavanaugh might (or might not) find a sufficient special need for *national security*³ but he would also very likely hold that "metadata" (like CSLI) cannot be seized and searched on a warrantless basis for "normal law enforcement," *e.g. domestic crimes*.

³ Hopefully counsel in any future case before him will cite to [*United States v. United States Dist. Court*](#), 407 U.S. 297, 320 (1972), which rejected a "special needs" exception to the warrant requirement in the context of wiretapping said to be necessary to national security. The Court there held "we do not think a case has been made for the requested departure from Fourth Amendment standards. The circumstances described do not justify complete exemption of domestic security surveillance from prior judicial scrutiny. Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech."

Is Information Privacy Threatened by Supreme Court Membership Turnover? (continued)

Judge Kavanaugh is not some law enforcement toady; to the contrary, he has a healthy distrust of governmental institutions and even law enforcement. For example, the Supreme Court accepted *certiorari* from the D.C. Circuit, which heard *Jones* at the intermediate level. He did not adopt the “mosaic” rationale used by the D.C. court to reverse the *Jones* conviction, but he did believe a warrant was necessary because law enforcement had trespassed on property as part of the search. Justice Scalia’s majority opinion in *Jones* expressly adopted Judge Kavanaugh’s Fourth Amendment analysis as the basis to affirm the D.C. Court’s outcome. In this respect, therefore, it appears that “Justice” Kavanaugh would likely align with the Scalia and Gorsuch Fourth Amendment perspective, which returns to the old property-based view, but recognizes that digital information has property implications.

We can be comfortable about “Justice Kavanaugh’s” potential disposition of a domestic criminal case like *Carpenter*. Those concerned about intrusions by national security apparatchiks, on the other hand, might not be pleased. It is always difficult to predict what will happen with appointees to the highest court, but it appears that, at worst, “Justice” Kavanaugh is likely to be a mixed bag.

The particular rationales may change, but the recent basic recognition of digital privacy as a “negative right” protecting against government intrusion will likely remain in place and might well advance even farther

The right to digital privacy as expressed in current Supreme Court precedent is probably secure and will hopefully advance regardless of who ends up occupying those nine important chairs.