Beyond the Fourth Amendment: Additional Constitutional Implications Arising From Big Government's Surveillance and Seizures of U.S. Citizens' Digital Property

The NSA has an electronic dragnet. The SEC wants an "agency exception" to the need for a warrant to obtain stored electronic data so they can more easily administer their civil enforcement duties. The Healthcare.gov website requires users to supply sensitive private information before the user can determine eligibility or shop for insurance plans, and this information is shared with a host of other federal agencies and can be used for virtually any purpose. Despite recent revelations about abuse, the IRS is now in charge of receiving and safeguarding more private information, and for more programs, than ever before. The Consumer Financial Protection Bureau is trying to make financial institutions disclose sensitive user transaction and purchasing history. The list goes on. Through these efforts the government is surreptitiously or publicly expanding its surveillance of US citizens in many ways, and trying to extensively gather private information that has historically been out of its reach except through a criminal warrant or voluntary, knowing disclosure. The government often goes to private third party service providers to obtain individuals' customer data, transactional data and even content, rather than going to the individual. This all-encompassing Big Government/Big Data[1] mining must stop. Individually and collectively these efforts give rise to police-state concerns; they threaten individual liberty and property and violate the Constitution.

Two examples of the government's hunger for intelligence on its own citizens have received the most discussion: NSA's activities and the effort by federal regulatory agencies to obtain content from service providers for civil enforcement purposes. While this paper will address only these two, similar concerns arise from other efforts as well.

Most of the commentators addressing the recent revelations of cybersurveillance by the NSA and other entities have focused on whether mass/bulk collection of users' communications-related information (both "metadata"[2] and/or content[3]) violates the

---

[1] Those who believe in a limited government should contemplate the proposition that in order for big government to operate with any kind of effectiveness it must have big data. Without this ocean of information big government would crumble and fall.

[2] The term "metadata" is not defined in any relevant statute. Some have described "telephony metadata" as including "comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call." "Internet metadata" has included "digital network information" such as connect times, email addresses and IP numbers, among other things. But there is no comprehensive explanation of what "metadata" is and is not. If one were to search for a statutory root for what has been described to date then "telephony" and "Internet" "metadata" information would be a combination of the data covered by 50 U.S.C. 1842(d)(2)(C)(i)(III), (V) and (VI) and (i)(III) and the information gleaned from a "pen register" and/or "trap and trace" authorized in 50 U.S.C. 1805(i), 1842(d)(2)(A)(iii), 1842(d)(2)(C)(i)(III), (V), (V) and 1842(d)(2)(C)(ii)(III). Note that

Fourth Amendment prohibition of "unreasonable searches and seizures" and its requirement that no "warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Mass/bulk collection has significant Fourth Amendment implications, but there are other as-yet ignored Constitutional issues.

Similarly, the ongoing efforts to update the Electronic Communications Privacy Act so it better reflects current technology, services and expansion of "the cloud" have hit a snag: several federal agencies, led by the Securities and Exchange Commission, want the ability to directly obtain the content of users' communication from service providers in the civil context, without any showing of probable cause that a crime has been committed and without having to meet basic Fourth Amendment "particularity" requirements concerning the place to be searched and the things to be seized. Many others have opposed these efforts, and Data Foundry agrees with them. But once again, another set of important Constitutional issues have been overlooked in the debate.

USERS' DIGITAL CONTENT IS "PROPERTY" PROTECTED BY THE FIFTH, NINTH, AND TENTH AMENDMENTS; THERE ARE FIRST AND SECOND AMENDMENT ISSUES AS WELL

The ability to own property and exercise the bundle of rights that comes with a property interest is one of the fundamental ways our society exercises liberty. The Fifth Amendment provides that no person may be "deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

A "property right" carries with it the right of dominion. It is the right, which a person has, as against all others, to the exclusive control, use, and enjoyment of any particular thing. This includes acquisition and disposal, the right to exclude others, a right against trespass and a right of quiet enjoyment. Interference with this right of dominion over personal property constitutes a trespass to chattel,[4] and can be a conversion under

---

under 50 U.S.C. 1812 the government may also independently obtain information under Title 18 chapters 119, 121, and 206. Those authorities contain roughly synonymous definitions with regard to this issue. *See*, *e.g.*, 18 U.S.C. 2703(c)(2)(C) and (E) and 18 U.S.C. 3127(3) and (4).

[3] 18 U.S.C. 2710(8) defines "contents" to mean "any information concerning the substance, purport, or meaning" of a communication.

[4] The government may make a copy without consent or require that a copy be made by a third party bailee Even if the original remains in place a nonconsensual duplication of the original is an exercise of dominion. For example, making a digital copy of the original is an infringement (akin to a taking) on the user's property rights in the intellectual property realm. Further, it is a trespass to chattel since there is a physical touching of the property, albeit in electronic form, as a necessary prerequisite to making the copy or otherwise obtaining the information. *See CompuServe, Inc. v. Cyber Promotions, Inc*., 962 F. Supp. 1015, 1021 (SD Ohio 1997*); Intel Corp. v. Hamidi*, 94 Cal. App. 4th 325 (Cal. App. 3d Dist. 2001); *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559, 1566, n. 6, 54 Cal. Rptr. 2d 468 (1996); Restatement (Second) of

certain circumstances. The interference need not completely destroy exclusivity in order to be actionable.

Users' digital content is property.[5] If you take a picture with a digital camera you own the resulting image file, just as you would an old-style Polaroid. If you do your diary using Microsoft Word© the electronic document is the modern equivalent of "papers", just as it would be if you had handwritten the words on paper and placed the book in a secure location in your house. No one would seriously contend that the government can forcibly or surreptiously enter your home or place of business and seize the digital content (for example, document or image files) on your computer hard drive. Nor would anyone legitimately assert that the government can cut a lock off of a storage unit or safety deposit box you have rented from a third party and confiscate or copy all of the digital that may have been placed in the rented space. If you are transporting computer disks from your home to the storage using your truck the government cannot just stop the vehicle, rummage through it and traipse away with the disks and information. The government cannot lawfully conceal itself in your house, truck[6] or rental unit and make a surreptitious digital copy[7] so as to listen in – unless it meets constitutional due process and probable cause requirements.

Torts §217b and Comment e, (1963 and 1964) [trespass to chattel includes the intentional use or "intermeddling" with a chattel in the possession of another].

[5] The courts have recognized this property interest, and the legal protection that flows therefrom: "Like the tort of trespass, the Stored Communications Act protects individuals' privacy and proprietary interests. The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, *cf.* Prosser and Keeton on the Law of Torts § 13, at 78 (W. Page Keeton, 5th ed. 1984), the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-1073 (9th Cir. Cal. 2004).

[6] *See*, *e.g.*, U.S. v. Jones, 132 S.Ct. 945, 950, n. 3 (2012) (emphasis added):

> Justice Alito's concurrence (hereinafter concurrence) doubts the wisdom of our approach because "it is almost impossible to think of late-18th-century situations that are analogous to what took place in this case." *Post, at ___, 181 L. Ed. 2d, at 928* (opinion concurring in judgment). But in fact it posits a situation that is not far afield--a constable's concealing himself in the target's coach in order to track its movements. *Ibid.* There is no doubt that the information gained by that trespassory activity would be the product of an unlawful search--whether that information consisted of the conversations occurring in the coach, or of the destinations to which the coach traveled. In any case, it is quite irrelevant whether there was an 18th-century analog. Whatever new methods of investigation may be devised, our task, at a minimum, is to decide whether the action in question would have constituted a "search" within the original meaning of the *Fourth Amendment*. Where, as here, the Government obtains information by physically intruding on a constitutionally protected area, such a search has undoubtedly occurred.

[7] Trespassing and then making a copy without permission clearly interferes with the owner's possessory interest. *See Jones*, 132 S.Ct. 951: "…a seizure of property occurs, not when there is a trespass, but "when

In today's world, "the cloud" is the equivalent of a storage unit. The Internet is the equivalent of the road, and electronic communications are modern day conveyors of content – the truck on the road to the storage unit. The user and the cloud storage providers have a bailor/bailee relationship. The user (bailor) does not waive any property interest. The cloud storage provider (bailee) has the right, indeed perhaps even the duty, to protect the information/property from governmental intrusion.[8]

The government's vast domestic electronic surveillance and the SEC's efforts to have an "agency exception" threaten individual liberty and property, and are contrary to constitutional principles. They erode privacy, impede legitimate business activities, have led to immense domestic and international economic impacts and are wholly antagonistic to the founders' intent and vision.

Data Foundry agrees that information content is the modern manifestation of the "papers and effects" protected by the Fourth Amendment. But it is also "property" for purposes of the Fifth, Ninth, and Tenth Amendments. Surveillance and seizure of digital information also implicates several aspects of the First Amendment, and it could impact the Second Amendment as well. Each of these Amendments form the basis of the "zones of privacy" held by all citizens, including business,[9] as against any governmental

---

there is some meaningful interference with an individual's possessory interests in that property." *Post, at ___, 181 L. Ed. 2d, at 927* (internal quotation marks omitted). Likewise with a search. Trespass alone does not qualify, but there must be conjoined with that what was present here: an attempt to find something or to obtain information." *See also Id*. at 953 (stating that seizure or monitoring of "electronic signals" that is not accompanied by a trespass is subject to *Katz* "expectation of privacy" analysis, but reserving question on result if there *is* a trespass on an "electronically signaled" "effect." *See also* 132 S.Ct. at 955 (Sotomayor, J concurring): "When the Government physically invades personal property to gather information, a search occurs."

[8] A bailee has the right – and often the duty – to exclude others from possession of the property entrusted to him. See generally Dobie, Handbook on the Law of Bailments and Carriers § 61, at 133 (1914) (right); id. § 65, at 157-58 (duty); Story, Commentaries on the Law of Bailments § 422a, at 421 (4th ed. 1846) (right); *id*. § 457, at 465-66 (duty). "As to everybody except the true owner of" the bailed property, the bailee "has the right of the owner to have and defend its custody and direct possession." See generally 4 LaFave, Search and Seizure § 11.3(f), at 344 (2d ed. 1987) ("person who is not the owner of the container but who possesses it by virtue of his status as bailee certainly has standing to object to illegal interference with his possessory interest"). *Foulke v. New York Consolidated Railroad Co*., 228 N.Y. 269, 275, 127 N.E. 237 (1920). Further, the bailee, whether gratuitous or for hire, has some duty of care. *See, e.g*., *Voorhis v. Consolidated Rail Corp*., 60 N.Y.2d 878, 879, 470 N.Y.S.2d 364, 365, 458 N.E.2d 823 (1983) (gratuitous bailee must avoid gross negligence; gross negligence presumed from nonreturn of property); *Aronette Manufacturing Co. v. Capitol Piece Dye Works, Inc*., 6 N.Y.2d 465, 468, 190 N.Y.S.2d 361, 364, 160 N.E.2d 842 (1959) (bailee for mutual benefit must exercise ordinary care).

[9] Although corporations are not entitled to the constitutional protections accorded to "citizens" they are "persons" for many (albeit perhaps not all) of the liberty protections afforded by the Constitution. For example, the U.S. Supreme Court long ago held that corporations and businesses are entitled to the procedural and substantive due process protections of the Fifth and Fourteenth Amendments. *Sinking Fund Cases*, 99 U.S. 700, 719 (1879); *Smyth v. Ames*, 169 U.S. 466, 522, 526 (1898); *Grosjean v. American*

intrusion or confiscation. The government may not seize user content without due process of law and just compensation.

- Fifth Amendment. The Fifth Amendment prohibits deprivations "of life, liberty, or property, without due process of law"; "nor shall private property be taken for public use, without just compensation." This Amendment ensures that citizens have a right to procedural and substantive "due process" as against the federal government in the civil context. It is a "taking" when a governmental entity captures a digital copy of user content while in transit on the Internet, or somehow acquires it while in storage. The user has a right to civil and/or criminal due process and must receive just compensation for the confiscation since the government has effectively deprived the user of his or her property or at least the exclusive right of dominion over and use of it.

- Ninth Amendment. The Ninth Amendment was inserted to re-emphasize the founders' desire for a federal government with limited scope and to make clear that all powers not granted were withheld by the people and reserved to them. The Ninth Amendment has been characterized as a "constitutional 'saving clause"'[10] This Amendment forms one of the so-called "penumbral" sources of a Constitutional right to privacy.[11] The framers might not be able to understand the technology behind the government's ongoing domestic surveillance and its efforts to avoid due process and compensation for taking digital property, but they could surely recognize its implications. Although there may be some statutory basis to some extent, nothing in the Constitution expressly authorizes or even contemplates this exercise of power in the absence of war or domestic insurrection, and this is especially so when most of the domestic information captured in the government's vast surveillance net has no relationship to terrorism or international intrigue, and certainly not to any crime. It is a classic case of overbreadth. Similarly, the effort to secure an "agency carve-out" that would allow an agency to seize digital property held by third party bailees over the objection of the bailor who owns the proerty cannot be squared with any power granted to the federal government. Both efforts are barred by to the Ninth Amendment.

- Tenth Amendment. Like the Ninth Amendment, the Tenth Amendment was promulgated to make clear that the federal government has only those powers expressly

---

Press Co., 297 U.S. 233, 244 (1936) ["a corporation is a 'person' within the meaning of the equal protection and due process of law clauses]. *See also Citizens United v. Federal Election Commission*, 558 U.S. 310, 342-356 (2010) (reaffirming that corporations entitled to First Amendment free speech protection, and overruling recent contrary holdings).

[10] *Richmond Newspapers v. Virginia*, 448 U.S. 555, 579–80 & n.15 (1980). *See also* The Rights Retained by the People: The History and Meaning of the Ninth Amendment © George Mason University Press, 1989.

[11] *See*, *e.g. Griswold v. Connecticut*, 381 U.S. 479, 484-486 (1965); *also Id.* at 487-499 (Goldberg, J concurring).

granted elsewhere in the Constitution; all other rights and powers are reserved to the people or (as with the Tenth), the states. Both Amendments in large part represent the constitutional equivalent of the judicial interpretative doctrine of *inclusio unius est exclusio alterius*. But they also have substantive import, particularly when other constitutional interests are involved, such as the Fifth Amendment and the First and Second Amendments (discussed below).[12] While Congress and the Executive Branch have express powers related to surveillance as it pertains to international matters, domestic surveillance does not fall within any of the federal governments enumerated powers. Put another way, nothing in the Constitution allows the federal government to engage in cyber-trespassing; it seems beyond peradventure that nothing in the Constitution justifies or allows the federal government engage in secretive trespass and then go on to purloin (through trespass or conversion) citizens' digital property without meaningful due process or any effort to compensate for the property deprivation.

- First Amendment. Government cybersurveillance directly threatens core First Amendment associational and expressive rights. Each person has the right to speak, and to individually decide the audience to whom the person is directly speaking.[13] If the citizen is aware of the monitoring he or she will likely reduce his or her expression and associational activities.[14] Surreptitious monitoring can unlawfully intrude on core expressive and associational rights, including those that have separate Constitutional protection such as the right to bear arms along with other statutory legal protections in the privacy area.[15]

---

[12] *See United States v. Lopez*, 514 U.S. 549, 589, 592-3 (1995) [Tenth Amendment one basis for striking down federal statute outlawing possession of guns in school zone] and *Printz v. United States*, 521 U.S. 898 (1997) [Tenth Amendment prohibits federal statute conscripting state officials into enforcement of federal gun regulatory regime.]

[13] A person conveying confidential or private information to a chosen recipient cannot have a constitutionally enforceable expectation that the recipient will not further disseminate the message. *See United States v. Miller*, 425 U.S. 435, 433 (1976). But reconveyance by an intended recipient is much different than secret interception by an unknown governmental body during conveyance or surreptitious access to and appropriation of information (property) in storage.

[14] *See Jones, supra,* 132 S.Ct. at 956 (Sotomayor, J concurring):

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring--by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track--may "alter the relationship between citizen and government in a way that is inimical to democratic society." *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (CA7 2011) (Flaum, J., concurring).

[15] *See* National Rifle Association *amicus curiae* brief, *ACLU, et al v. Clapper, et al*, No. 13-cv-03994 (WHP), S.D.N.Y, Document 44-1 (September 4, 2013).

CONCLUSION

The government's ongoing efforts to pervasively monitor citizens' through electronic monitoring, interception and by gathering electronic information from third party bailees intrude on individual liberty and property, and violate the Constitution's due process, property, privacy, expression and associational rights. Congress must act before we turn into a full-blown surveillance state.