THE THIRD AMENDMENT, PRIVACY, AND MASS SURVEILLANCE

Steven I. Friedland

"The world isn't run by weapons anymore, or energy, or money. It's run by little ones and zeroes, little bits of data. It's all just electrons."[1]

We live in an era of mass surveillance. Advertisers, corporations and the government engage in widespread data collection and analysis, using such avenues as cell phone location information, the Internet, camera observations, and drones. As technology and analytics advance, mass surveillance opportunities continue to grow.[2]

The growing surveillance society is not necessarily harmful[3] or unconstitutional. The United States must track people and gather data to defend against enemies and malevolent actors. Defenses range from stopping attempts to breach government computers and software programs,[4] to identifying and thwarting potential terroristic conduct and threats at an embryonic stage.

Yet, without lines drawn to limit mass data gathering, especially in secret, unchecked government snooping likely will continue to expand. John Kerry, the sitting Secretary of State, even recently acknowledged that the government has "sometimes reached too far" with its surveillance.[5] The stakes for drawing lines demarcating

---

1. SNEAKERS (Universal Pictures 1992).

2. *See, e.g.*, Quentin Hardy, *Big Data's Little Brother*, N.Y. TIMES, Nov. 12, 2013, at B1 ("Collecting data from all sorts of odd places and analyzing it much faster than was possible even a couple of years ago has become one of the hottest areas of the technology industry. . . . Now Big Data is evolving, becoming more "hyper" and including all sorts of sources.").

3. *Contra* Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 *passim* (2013) (arguing that surveillance is a direct threat to "intellectual privacy," or the notion that ideas develop best in private).

4. China allegedly attempts to hack U.S. computers on a daily basis. *See* Keith Bradsher, *China Blasts Hacking Claim by Pentagon*, N.Y. TIMES (May 7, 2013), http://www.nytimes.com/2013/05/08/world/asia/china-criticizes-pentagon-report-on-cyberattacks.html.

5. Mark Memmott, *U.S. Spying Efforts Sometimes 'Reached Too Far,' Kerry Says*, NAT'L PUB. RADIO (Nov. 1, 2013), http://www.npr.org/blogs/thetwo-way/2013/11/01/242288704/u-s-spying-efforts-sometimes-reached-too-far-kerry-says (quoting John Kerry as saying that "some of the electronic surveillance programs of the National Security Agency have been on 'automatic pilot' in recent years and have inappropriately 'reached too far'"). Google's Executive Chairman, Eric Schmidt, was less restrained about secret government spying, calling reports of National Security Agency ("NSA") interception of the main communication

privacy rights and the government's security efforts have never been higher or more uncertain.

This Article argues that the forgotten Third Amendment, long in desuetude, should be considered to harmonize and intersect with the Fourth Amendment to potentially limit at least some mass government surveillance. While the Fourth Amendment has been the sole source of search and seizure limitations, the Third Amendment should be added to the privacy calculus,[6] because it provides a clear allocation of power between military and civil authorities and creates a realm of privacy governed by civil law.

Consequently, in today's digital world it would be improper to read the words of the Third Amendment literally, merely as surplusage. Instead, the Amendment's check on government tyranny should be viewed as restricting cybersoldiers from focusing surveillance instrumentalities[7] on and around private residences or businesses in an intrusive way—or using proxies to do so—that would serve as the functional equivalent of military quartering in the civil community.

I. MASS SURVEILLANCE

Imagine an America with continual domestic drones, which collected camera and cell phone surveillance of every person in a particular residential subdivision, business headquarters, or city high-rise building. The surveillance would be mostly secret but "in public," capturing people sitting on rocking chairs on their front porches, unloading bags of groceries from their cars, opening their wallets to pay bills, and anything visible through windows in private residences and businesses. People who go to sporting events or the supermarket would have their faces matched to an existing database. The metadata from Internet use, cell phone location data and other sources, including hyper-local observations, would be fed into computers for complex analysis and combined with other surveillance

links used by Google and Yahoo to connect to their data centers "outrageous." *See* Eyder Peralta, *Google's Eric Schmidt Says Reports of NSA Spying 'Outrageous'*, NAT'L PUB. RADIO (Nov. 4, 2013), http://www.npr.org/blogs/thetwo-way/2013/11/04/242960648/googles-eric-schmidt-says-reports-of-nsa-spying-are-outrageous ("There clearly are cases where evil people exist, but you don't have to violate the privacy of every single citizen of America to find them.").

6. For the dual rationales of the Amendment, see Geoffrey M. Wyatt, *The Third Amendment in the Twenty-First Century: Military Recruiting on Private Campuses*, 40 NEW ENG. L. REV. 113, 122–24 (2005).

7. Instrumentalities do not include malware such as the "Stuxnet" computer worm, tracking devices, cookies and more. The Stuxnet worm was allegedly used by several countries to infiltrate and infect Iran's nuclear facilities. *See* Alan Butler, *When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy*, 62 AM. U. L. REV. 1203, 1204–05 (2013).

information.[8] This information, all gathered and utilized outside the private space protected by the physical walls and doors of houses, would present a fairly intimate picture of these individuals over time, creating in essence a virtual window to what is occurring within the house or building, as well as without.[9]

Such a day is not far off. Drones and robots are currently being employed domestically in the skies,[10] on land, and in the seas[11] for various purposes, although apparently not yet on a continual and widespread basis. Yet, expansion of their use seems inevitable.[12] While most unmanned aircraft systems fly high overhead, out of sight, as more information is released and people look more carefully, we will know they are there. The government also is developing the Biometric Optical Surveillance System ("BOSS"), which will have tremendous capabilities for identifying people from distances of up to 100 meters. This system was scheduled for testing at a public hockey game in the State of Washington in 2013.[13] To supplement the information acquired directly, the government obtains considerable amounts of information through the consent of third parties.[14]

While surveillance is not overly intrusive when deployed in public places, where being watched can be expected, it still can be dangerous.[15] Surveillance, when taken as a whole with information

---

8. Indeed, the NSA alone gathers 20 billion "record events" per day. James Risen & Laura Poitras, *N.S.A. Examines Social Networks of U.S. Citizens*, N.Y. TIMES, Sept. 29, 2013, at A1.

9. This off-the-wall versus through-the-wall distinction was advanced in *Kyllo v. United States*, 533 U.S. 27 (2001), where the Court found that the police unconstitutionally used an infrared heat detection device to determine whether heat lamps were being used in the house to grow marijuana. *Id.* at 40.

10. In fact, Robert Mueller, the current F.B.I. Director, recently conceded at a Senate hearing that drones indeed have been used for some "very minimal" domestic surveillance operations. Phil Mattingly, *FBI Uses Drones in Domestic Surveillance, Mueller Says*, BLOOMBERG (June 19, 2013), http://www.bloomberg.com/news/2013-06-19/fbi-uses-drones-in-domestic-surveillance-mueller-says.html.

11. William Herkewitz, *Ocean Drones Plumb New Depths*, N.Y. TIMES, Nov. 12, 2013, at D1.

12. M. Ryan Calo, *The Drone As Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29, 30–31 (2013). Calo notes that there are several counties where drone use is occurring; however, there are also several restrictions that limit use of drones. *See* Operation and Certification of Small Unmanned Aircraft Systems (SUAS), 76 Fed. Reg. 40,107, 40,107–08 (July 7, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-07-07/pdf/2011-15494.pdf#page=16.

13. Eddie Keogh, *DHS to Test Facial Recognition Software at Hockey Game*, RUSS. TODAY (Sept. 18, 2013), http://rt.com/usa/dhs-hockey-washington-face-033/.

14. Another way the government obtains information is through warrants and requests under FISA. *See* Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1885 (2010).

15. *See* Neil Richards, *supra* note 3, at 1952–58. Professor Richards organizes his argument as follows: "Part II shows how surveillance menaces our intellectual privacy and threatens the development of individual beliefs in ways that are inconsistent with the basic commitments of democratic societies. Part III explores how surveillance distorts the power relationships between the

and data gathering, can form a mosaic of intrusion in a manner similar to that described by Justices Alito and Sotomayor in their concurrences in the GPS tracking device case *United States v. Jones*.[16] Pursuant to this "mosaic theory," a privacy violation does not require a physical trespass. One commentator noted the following:

> Today's police have to follow hunches, cultivate informants, subpoena ATM camera footage. . . . Tomorrow's police . . . might sit in an office or vehicle as their metal agents methodically search for interesting behavior to record and relay. Americans can visualize and experience this activity as a physical violation of their privacy.[17]

Significantly, surveillance also is an expression of power—an accumulation of data that can be used against persons, even creating that intimate picture of what occurs inside a house when the cybersleuth never actually sets foot in it. As another commentator has observed about possible power abuses, "We cannot have a system, or even the appearance of a system, where surveillance is secret, or where decisions are made about individuals by a Kafkaesque system of opaque and unreviewable decision makers."[18]

II. THE THIRD AMENDMENT'S PLACE IN CONSTITUTIONAL ORTHODOXY

"[N]o Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."[19]

---

watcher and the watched, enhancing the watcher's ability to blackmail, coerce, and discriminate against the people under its scrutiny." *Id.* at 1936.

16. 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring); *Id.* at 961 (Alito, J., concurring). The case involved the placement of a GPS device on a private individual's car. *Id.* at 948 (majority opinion). Writing for the majority, Justice Scalia found that the installation of the device was a search within the meaning of the Fourth Amendment. *Id.* at 952.

17. Calo, *supra* note 12, at 32.

18. Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. ONLINE 41, 43 (2013). The authors discuss the paradox of power associated with Big Data, stating that "[b]ig data will create winners and losers, and it is likely to benefit the institutions that wield its tools over the individuals being mined, analyzed, and sorted. Not knowing the appropriate legal or technical boundaries, each side is left guessing. Individuals succumb to denial while governments and corporations get away with what they can by default, until they are left reeling from scandal after shock of disclosure." *Id.* at 45.

19. U.S. CONST. amend. III.

A. Origins and Interpretations

The Third Amendment might have an obscure[20] and obsolete[21] place in constitutional law orthodoxy, yet it draws on a rich history. The bright-line Amendment[22] traces its origins to pre-revolutionary war England, where multiple abuses by the king in quartering soldiers, the Royal entourage and their horses in private residences led to laws prohibiting quartering in England.[23] These laws were enacted in part to avoid maintaining a standing army, especially during peacetime.[24] For example, in 1689, the British Parliament enacted the Mutiny Act, which outlawed the quartering of troops in private homes without the owner's consent.[25] A standing army was thought to provide a slippery slope to tyranny, and it was the confluence of military with civil authority that was the real problem, not simply the taking of private resources by the King.

Continued quartering abuses in the colonies led to the adoption of the Third Amendment. Patrick Henry argued for the amendment because it offered rule by civil authority, not military force,[26] as did Samuel Adams, who objected to soldiers quartered "in the body of a city" and not just houses.[27]

Perhaps the amendment's desuetude is attributable in part to the fact that it has only been the subject of Supreme Court cases in passing, such as in *Griswold v. Connecticut*,[28] and just one significant direct judicial interpretation, *Engblom v. Carey*,[29] a 1981 Second Circuit Court of Appeals case. In *Engblom*, the court was confronted

---

20. William S. Fields & David T. Hardy, *The Third Amendment and the Issue of the Maintenance of Standing Armies: A Legal History*, 35 AM. J. LEGAL HIST. 393, 429 (1991).

21. Morton Horwitz, *Is the Third Amendment Obsolete?* 26 VAL. U. L. REV. 209 *passim* (1991).

22. This provision firmly states its singular prohibition. Interestingly, it still arguably has been violated on multiple occasions. *See, e.g.*, B. Carmon Hardy, *A Free People's Intolerable Grievance*, *in* THE BILL OF RIGHTS, A LIVELY HERITAGE 67, 69 (1987); Tom W. Bell, *"Property" in the Constitution: A View From the Third Amendment*, 20 WM. & MARY BILL RTS. J. 1243, 1276 (2012).

23. *See, e.g.*, B. Carmon Hardy, *A Free People's Intolerable Grievance – The Quartering of Troops and the Third Amendment*, 33 VA. CAVALCADE 126 (1984); J. Alan Rogers, *Colonial Opposition to the Quartering of Troops During the French and Indian War*, 34 MIL. AFF. 7, 7–11 (1970).

24. Fields & Hardy, *supra* note 20, at 395; Hardy, *supra* note 23; Rogers, *supra* note 23.

25. Horwitz, *supra* note 21, at 210.

26. Patrick Henry, Patrick Henry's Objections to a National Army and James Madison's Reply, Virginia Convention (June 16, 1788), *in* 2 THE DEBATE ON THE CONSTITUTION 695, 696–97 (Bernard Bailyn ed., 1993).

27. Samuel Adams, Letter to the Editor, Bos. Gazette, Oct. 17, 1768, *reprinted in* 5 THE FOUNDERS' CONSTITUTION 215, 215 (Philip B. Kurland & Ralph Lerner eds., 1987) ("No man can pretend to say that the *peace* and *good order* of the community is so secure with soldiers quartered in *the body of a city* as without them.").

28. 381 U.S. 479, 484 (1965) (discussing the Third Amendment as a part of the penumbras forming a constitutional privacy right).

29. 677 F.2d 957 (2d Cir. 1982).

with a claim by two correctional officers who claimed their Third Amendment rights were infringed by the State of New York when the state quartered national guardsmen in their dormitory-style residences during a prison strike by the guards in an upstate New York prison.[30] The guards were renting their rooms from the State.[31]

The court first applied the Third Amendment to the State of New York through the incorporation doctrine of the Fourteenth Amendment.[32] Significantly, the court viewed several of the key terms in the amendment expansively. The court considered the national guardsmen to be "soldiers" and held that the Third Amendment applied to the guardsmen as "tenants," even if they did not own their quarters, despite the express language in the amendment.[33]

B. The Relationship Between the Third and Fourth Amendments

The Second Circuit in *Engblom* also used an analysis borrowed from the Fourth Amendment, setting forth a standard of a "legitimate expectation of privacy" to determine if Third Amendment rights were triggered.[34] It noted that the amendment's objective was to protect the fundamental right to privacy in conjunction with the use and enjoyment of property rights.[35]

The *Engblom* analysis at least implicitly recognized the interlocking nature of the Third and Fourth Amendments and the primary role of the Fourth Amendment as the privacy standard bearer. As one noted commentator observed, "If the Fourth Amendment had never been enacted, the Third Amendment might have provided the raw material for generating something like an anti-search and seizure principle."[36]

Constitutionally, courts have used the Fourth Amendment to protect against government snooping on others, but the Fourth Amendment has been strapped with textual limits, given its language protecting only against unreasonable, not all, searches and seizures, and interpretive limits authored by a reticent Supreme Court that has stuck by rules created in predigital cases.[37] Also, while the

30. *Id.* at 958–59.
31. *Id.* at 959–60.
32. *Id.* at 961.
33. *Id.* at 961–62.
34. See William Sutton Fields, *The Third Amendment: Constitutional Protection from the Involuntary Quartering of Soldiers*, 124 MIL. L. REV. 195, 207 & n.108 (1989); Ann Marie C. Petrey, Comment, *The Third Amendment's Protection Against Unwanted Military Intrusion*, 49 BROOK. L. REV. 857, 857–64 (1983).
35. *Engblom*, 677 F.2d at 962.
36. *See* Horwitz, *supra* note 21, at 214.
37. *See, e.g.*, the physical trespass test used in *United States v. Jones,* 132 S. Ct. 945, 950–52 (2012); *Id.* at 955 (Sotomayor, J., concurring) ("[T]he trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum."). The case involved the placement of a GPS device on a private individual's car. *Id.* at 948 (majority opinion). Justice Scalia found that doing so

Fourth Amendment protects against United States government spying, it does not apply to such conduct by foreign governments, which can and do swap data with the United States,[38] or apparent swaps of data with thousands of technology, finance, and manufacturing companies.[39]

Preoccupation with the Fourth Amendment doctrine, combined with a Gresham's Law style of constitutional application suggesting that general principles often end up marginalizing specific provisions, help explain the Third Amendment's disuse. A contextual interpretation of this amendment in the digital era could offer a significant link in a system of digital checks and balances.

III. INTERPRETATION

The Third Amendment's relevancy to surveillance privacy depends on its interpretation,[40] both in terms of its themes and words. The amendment's broad themes resonate in the world of "Big Data" and the Internet. The amendment provides a bright line allocation of power, with a clear distinction that limits the military and protects homes from intrusion without consent. As evidenced by Due Process, Equal Protection, and other constitutional doctrines such as the Eighth Amendment, the Court often takes into account evolving facts and cultural transformations over time. A more specific analysis of each component of the Amendment follows.

A. War and Peace

The wartime/peacetime distinction in the amendment provides a useful contrast about the expansiveness of government power at different times. When compared to the Fourth Amendment, the framers of the Third Amendment provided a clear line of what is reasonable in times of war or peace.

---

without a warrant unconstitutionally violated Mr. Jones's property rights. *Id.* at 949.

38. A prime illustration is the relationship between England and the United States. They have swapped sensitive data on each other's citizens, doing indirectly what is not permitted directly. *British Spy Agency Taps Cables, Shares with U.S. NSA – Guardian*, REUTERS (June 21, 2013), http://uk.reuters.com/article/2013/06/21/uk-usa-security-britain-idUKBRE95K10620130621.

39. Michael Riley, *U.S. Agencies Said to Swap Data with Thousands of Firms*, BLOOMBERG (June 15, 2013), http://www.bloomberg.com/news/2013-0614/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html.

40. Most scholars believe that words in the Constitution require interpretation. Originalism, for example, looks to ground the meaning of the words based on the era and its sources. Construction can have varying levels of strictness. For example, Justice Scalia believes that "[w]ords have meaning. And their meaning doesn't change." Jennifer Senior, *In Conversation: Antonin Scalia*, N.Y. MAG. (Oct. 6, 2013) http://nymag.com/news/features/antonin-scalia-2013-10/.

B. Soldiers

History is instructive. Early English case law reflects the concern over forced accommodations and board not only by soldiers, but also by the royal court and its entourage.[41] The prohibition extended to the soldiers' instrumentalities, namely their horses.[42] In the late 1700s, soldiers honorably fought in uniform generally within full view of the enemy. Times have changed. In *Engblom*, national guardsmen were considered soldiers, even though they were defending a domestic prison. Today, the definition would certainly include cyber agents, military personnel who are paid to hack and disrupt another country's software and hardware and to protect our own. Instead of horses, these cyber soldiers use codes or metal instrumentalities to invade others' cyber spaces.[43] Using stealth and remote access to obtain and crunch data is the new face of warfare; these soldiers disrupt and disable various aspects of a country to keep it off balance and vulnerable. For example, deployment of the Stuxnet worm, placed on computers in Iran to disrupt its quest for nuclear weapons, is but one illustration of the new military.

C. Quartering

Quartering historically came to mean an "act of a government in billeting or assigning soldiers to private houses, without the consent of the owners of such houses, and requiring such owners to supply them with board or lodging or both."[44] Billeting can mean a letter ordering the assignment or the assignment itself. This definition yields some insights. Significantly, it is a military intrusion into home life—civilian life—by soldiers, which is why early English analysis incorporated the forced provision of board and the tethering of horses as part of quartering. Thus, it is the intrusion and diminishment of civil authority and life that matter, even if it is through remote access rather than the physical presence of the soldiers. An unmanned drone is the equivalent of a piloted plane. Would military personnel stationed regularly at businesses, or operating cameras on the rooftops of private residences or businesses, or even on all public mailboxes generate intimidation or intrusion into daily life? Would the intrusions still be significant if the soldiers were outside of the houses and businesses, in the curtilages, peering inside or the equivalent? Especially if seen or heard, electronic surveillance devices could significantly interfere with civilian community life and

---

41. Tom W. Bell, *The Third Amendment: Forgotten but Not Gone*, 2 WM. & MARY BILL RTS. J. 117, 121 (1993).

42. *Id.* at 123 n.46 (citing Coram Rege Roll, no. 564 (Easter 1402), m. 28d, at Westminster in Middlesex, *reprinted in* VII SELECT CASES IN THE COURT OF KING'S BENCH 121–23 (G.O. Sayles ed., 1971)).

43. See Butler, *supra* note 7, at 1231–33, for an argument that it does trigger the Third Amendment.

44. *Quartering Soldiers,* THE LAW DICTIONARY, http://thelawdictionary.org/quartering-soldiers/ (last visited Jan. 13, 2013).

intrude on civilian authority. As one commentator has noted, "[G]overnment or industry surveillance of the populace with drones would be visible and highly salient. People would *feel* observed, regardless of how or whether the information was actually used."[45]

Quartering today also can involve proxies, where the U.S. government knows and promotes the equivalent of private or foreign quartering for its own gain. One illustration of proxy quartering might involve an agreement between countries to swap sensitive data on each other's citizens, revealing the intricacies of civil life inside the cities and their residences or businesses.[46]

D. Any Houses

The term "any houses" on its face appears highly restrictive.[47] Yet, at least in *Engblom*, it also means tenancies. While tenancies refers to residences, today there are a proliferation of buildings housing businesses, which fall within the types of civil occupancies where sensitive and confidential civil life occurs. Invasions of these buildings without physical entry can occur regularly in the digital world, which is how the term should be judged and is in keeping with the intent of the framers.

While the term "any houses" could be more broadly construed to mean all private chattel or real property, including electronic devices,[48] this likely would expand the meaning of the amendment to become a version of the Fifth Amendment Takings Clause, not likely intended for the Third Amendment's "houses" distinction, particularly when the Fourth Amendment protects not only houses, but also "persons, places, and effects."

E. Without Consent

Although the amendment permits quartering in peacetime with consent, if quartering extends to businesses, the government-private business partnerships create questions about the voluntariness of the relationships. This is especially the case if the government inserts employees into the private business locations. This type of relationship might not generate adequate voluntary consent.[49]

---

45. Calo, *supra* note 12, at 33.

46. *See supra* note 38.

47. Given the rejection of an alternative Amendment that would have limited it only to private and not public houses, the Framers opted for a broader approach. *Compare* Bell, *supra* note 41, at 129 n.105, *with* U.S. CONST. amend. III.

48. A recent commentator has provided the Amendment with a similar construction. *See* Butler, *supra* note 7, at 1230.

49. The government also pays and partners with companies to produce and swap data. Riley, *supra* note 39.

CONCLUSION

The Third Amendment no longer will be the forgotten amendment if it is considered to interlock with the Fourth Amendment to provide a check on some domestic mass surveillance intruding on civil life, particularly within the home, business or curtilage of each. In the digital era, the dual purposes of the Amendment should be understood to potentially limit the reach of cyber soldiers and protect the enjoyment of a private tenancy without governmental incursion.