A NEW STANDARD FOR APPROPRIATION, WITH SOME REMARKS ON AGGREGATION

Joseph S. Fulda *

> It has been repeatedly decided that [the Fourth and Fifth] Amendments should receive a liberal construction, so as to prevent stealthy encroachment upon or "gradual depreciation" of the rights secured by them . . . In the spirit of these decisions we must deal with the questions before us.
>
> *Gouled v. United States*, 255 U.S. 298, 304 (1921)

The questions we consider surround appropriation of information, in particular what constitutes misappropriation of information as opposed to misappropriation of property containing information. As information is both emitted and captured without encapsulation in property — pure data — we need such a definition lest the Fourth Amendment and tort law alike become a dead letter, and privacy a quaint notion that like so many others our fathers held dear we will simply collectively forget.

Background

Long ago, when privacy meant security of one's person and property and a reputation that could only be damaged by probes in and of visible light or audible sound, it was enough to proclaim, with Sir Edward Coke, the great lawyer of sixteenth-century England, that "a man's house is his castle"[1] and that shielding this sanctuary would secure not only his person and property, but also his reputation.

---

* Joseph S. Fulda, C.S.E., Ph.D. is the author, most recently, of *Eight Steps towards Libertarianism* (Free Enterprise Press) and is a contributing editor of The Freeman, an Associate Editor of Sexuality & Culture, and a columnist for Computers and Society, in which an earlier version of this article appeared.

[1] Quoted in John Bartlett, *Familiar Quotations* 9th ed (:Little, Brown, and Company, 1901). The dictum has appeared or been alluded to in countless United States Supreme Court decisions, the most famous early allusion being in *Boyd v. United States*, 116 U.S. 616 (1886) (first announcing an exclusionary rule) and the most famous early appearance being in *Weeks v. United States*, 232 U.S. 383 (1914) (expanding the exclusionary rule significantly); but, its appearance dates back to a little-known (and rather unusual) trespass case in the nineteenth century: *Luther v. Borden*, 48 U.S. (7 How.) 1 (1849). The right of privacy as against the government has been principally, though not exclusively, shaped by criminal cases in which exclusion of evidence improperly appropriated was sought by the defendant.

To secure the former against seizure and the latter against search was, in both cases, to ward off physical intrusion of, in the words of the Fourth Amendment, the "persons, houses, papers, and effects" of the citizenry. In the world of the Founders, the two facets of the crown jewel of the common man's privacy in his castle could be secured with a single injunction.

All that was in contention was whether the latter of these securities was as critical and as essential for human life as the former. Robert Frost forever immortalized this dialogue in "The Mending Wall,"[2] his poem of two neighbors who talk past each other, the one saying simply and austerely "Good fences make good neighbors," the other arguing "'Why do they make good neighbors? Isn't it where there are cows? But here there are no cows . . . '" "He is all pine and I am apple orchard. My apple trees will never get across and eat the cones under his pines, I tell him."

Today, however, new technologies for searching out the private are constantly being developed and deployed. They probe more deeply, more widely, and much more softly than do traditional methods, transcending barriers such as walls and distance, darkness and time, and flesh and bones that have historically made such probing impossible. Our boundaries are increasingly permeable, as we master the science of imperceptible penetration by and reception of electromagnetic and acoustic waves of all frequencies, as well as streams of particulate matter, to track, trace, and home in on persons and their biophysical signals — heat, pressure, motion, brain waves, sound, perspiration, cellular residue, olfacients, waste matter — and as we integrate these largely unseen, unheard, and unfelt waves into revealing intelligence with modern computer and communications technology.[3]

If the privacy that has been compromised is the security of reputation, we must ask which of the three traditional torts for invasion of privacy is involved: appropriation — taking information; disclosure — revealing information; placement in a false light — arranging revealed information in such a way as to portray a picture that, on the whole, is false and damaging. The answer, unfortunately, is all three, but our concern here is with the first of these, appropriation. The previous paragraph gives a summary of just how much is new by way of appropriation.[4]

---

[2] Reprinted in its entirety in *The Columbia Granger's World of Poetry* (Columbia University Press, 1992).

[3] Much of this paragraph's wording is rephrased from Gary T. Marx, "Ethics for the New Surveillance," The Information Society 14 (July-August 1998): 171-185, at 171-172.

[4] For completeness we add that, with the Internet, disclosure has also changed as anyone with a modem and a PC can broadcast anything at all to millions at virtually no cost. Also changed is placement in a false light, as imaging and graphics techniques together with techniques for data mining and knowledge discovery have made misleading misrepresentations, whether of images, text, or numbers, easier and less costly to produce. We are not concerned here with these matters

The Standards

The first definition of appropriation was that appropriate for property, for, as we noted, it was necessary to invade person or property to invade privacy, hence to appropriate information was to forcibly trespass on real property or to take personal property by force. This is the definition adopted by the Court in its first wiretapping case, *Olmstead v. United States*, 277 U.S. 438 (1928). But as Justice Brandeis observed in his dissent,

> "Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet . . . The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions . . . Can it be that the Constitution affords no protection against such invasions of individual security?"[5]

A broader definition, never adopted by the Court[6], but also stemming from the law of property would be to prohibit, absent the Constitutional safeguards, access to information by force or fraud, which would rule out sting operations as a source of information, for example.

Instead, faced again with a case of wiretapping in *Katz v. United States*, 389 U.S. 347 (1967), the court unwilling to abide by *Olmstead* any longer announced that "[t]he rule that has emerged . . . is . . . first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'" at 361 (Harlan, J., concurring).[7] The problem with this

---

because they are not philosophical and do not require a change in definitional apparatus — the greater ease and lesser cost of committing wrongdoing affects not the definition of wrongdoing but the penalties levied for same.

[5] 277 U.S. at 473-474 (Brandeis, J., dissenting).

[6] At first glance, it might appear that just such a standard had been adopted in *Gouled v. United States*, 255 U.S. 298 (1921), but a careful reading shows that the concern was not that information had been gained by fraud—but that the property (papers) that contained the information was acquired by stealth instead of by forcible trespass. Chief Justice Taft was later to say, in writing for the court in *Olmstead* (277 U.S. at 468), that a true fraud standard could not be adopted for consequentialist reasons. In other words, the government relies so heavily on information obtained under false pretenses, prosecution of crime would be severely hampered by restricting the practice.

[7] It is not to be supposed that *Katz* simply overruled *Olmstead*. *Olmstead* was eroded by a long line of cases leading up to *Katz*. Nor was the decision in *Katz* unanimous. Justice Black, dissenting, pointed out that the Founders knew of such activities as eavesdropping and chose not to prohibit the government from gaining information this way. Wiretapping, he reasoned, was

approach is clear enough: It is what engineers term a positive feedback loop. The more privacy is invaded, the less reasonable it becomes to expect it, and the less reasonable it is to expect it, the more it may be invaded. The proper response to this flawed reasoning is simple enough: People often expect, in the sense of demand, what they cannot expect, in the sense of predict. We may thus have a right to expect our privacy to be respected in the former sense, whether or not we may expect it to be respected in the latter sense. Expectations, in other words, must be defined against a fixed standard of reasonableness, not one which is programmed to continuously decay.

But what standard? Above, we suggested one enhancement to the older theory of intrusion by force, intrusion by force or fraud. Elaborating on that idea, we state our central thesis: **Privacy is invaded, when any means are used that bypass the subject's consent as manifested by the subject's observable (i.e., objective) behavior, reasonably interpreted.**[8] Note that it does not matter if the behavior is effective; against modern technologies available to states and corporate entities, no individual can be expected to safeguard his own privacy. The behavior must simply be manifest. Verily, this does not answer the questions that will arise as cases reach the courts, for we do not say, and do not wish to say, what precisely is "behavior," what precisely is a "manifestation," and what precisely constitutes "bypassing" and we will certainly not hold forth on how to interpret behavior "reasonably." We simply state a reasonable, objective, and broad rule — typical of Constitution-level rules — and, in the usual fashion, leave it to the judicial canons of interpretation to fill in the details.

However, we do want to persuade the reader that this rule is, indeed, reasonable, objective, and broad enough to cover all technologies, including those that may be developed and deployed in the future. For this, we simply must have recourse to

---

simply advanced eavesdropping. The problem with this view is its theoretical nature. The Constitution of the United States grew out of the experience of the Founders and eavesdropping had not been a mode of law enforcement. Too often it would require trespass; too often the agents of the state would be caught at it. What had been modes of law enforcement, such as searches and seizures made pursuant to general warrants, and seen as invasion of privacy, were prohibited. The Founders did not prohibit invasions of rights that were not an issue in the Colonial experience. Justice Black also argued that the language of the Fourth Amendment compelled the conclusion that tangible objects and actual places were being discussed, to which almost the same rejoinder applies. What nature made difficult, and the colonists did not have any experience of, was not to end up prohibited by the Bill of Rights.

[8] This approach is hinted at in *Katz*, though certainly not adopted there. The key quote is "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. ... But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (389 U.S. at 351) Change "may be" to "is" and that is our standard. I wish to thank Professor Gary T. Marx and Professor Chuck Huff for reminding me of the importance of objectivity not only in observation, but also in interpretation, of behavior—hence "reasonably interpreted."

details. So we will examine several cases that have been hinted at earlier in this article, and consider some additional relevant cases as examples. The reader is left to decide for himself the intellectual strength of the standard we propose both by its theoretical appeal and by some of its practical consequences as we would apply the theory to practice.

Examples

We now consider some of the examples from earlier in this paper: signals coming from heat, pressure, motion, brain waves, sound, perspiration, cellular residue, olfacients, waste matter. Heat: This has been an issue as infrared radiation, a sign of heat, can be detected. Position: Collecting this information on persons in public streets, byways, and open spaces is permissible, but collecting it through homes and cars and other spaces which are often temperature-controlled bypasses the consent of the subject whose behavior — being behind walls and conditioning the temperature — is reasonably interpreted as at odds with nonconsensual collection. (And never mind that these steps do not successfully prevent such collection.)

Pressure and motion: These can be detected by sensors alert to air streams, video cameras used for surveillance, toll collection systems, and the like. Position: If the video cameras, motion and pressure sensors, or toll systems are known to the person being watched and he can evade them — i.e., not all lanes have such a sensor, not all areas are under surveillance — then his failure to evade these technologies is tacit consent. Hidden cameras and sensors, on the other hand, clearly bypass consent as[9] manifested by the freewheeling way people walk about and drive around. Human beings who are watched act warily, even furtively, to avoid being watched. The absence of this typical guarded attitude and the presence of the more usual unguarded motion is manifest. To draw a distinction, no such comparable behavioral manifestation is present when heat is or is not monitored.

Brain waves: As electrical currents, Justice Brandeis' worry may one day become a reality. There is no reason, in principle, why a complete map of all electrochemical activity in the brain together with a map of the person's brain itself should not yield up one's thoughts. Position: Once such technology becomes available in the distant future,

---

[9] We say "distant future" and "in principle" bearing in mind the following passage from Rosalind W. Picard, *Affective Computing* (MIT Press, 1997), p. 39: "I have heard some people suggest that science might be able to find a process of recovering somebody's thoughts by looking at various brain signals produced while thinking those thoughts. This recovery problem may be posed as a so-called "inverse problem," where the goal is to invert the signal generation process to reconstruct the thoughts that gave rise to the signals. However, inverse problems are notoriously difficult. Thought-reading may be the biggest "inverse problem" imaginable. In other words, people need not worry about any person or machine reading their ... thoughts."

you can be sure people will frantically demand a shielding counter-technology (which should be much easier to develop), which, even if it can be circumvented — even relatively easily — will suffice, if used, to render such thought probing illicit. More likely, however, there will be a frantic demand for broad prohibiting legislation or a Constitutional Amendment, rendering reliance on the Fourth Amendment — which would allow such probes with a warrant based on probable cause (although it is likely that the Fifth Amendment would preclude the government from using such probes in court[10]) — unnecessary.

Sound: As receivers become more powerful and their resolution is enhanced, this has become a consideration for ordinary conversations (advertisements for snooping devices that pick up sound at a distance have made it into the back of comic books), as well as conversations on cordless phones, cellular phones, PCS phones, and Internet telephony and e-mail. Position: The monitoring of ordinary bodily sounds or speech (such as song) made aloud and to oneself in public is not protected; the case is akin to heat. But conversations with others, however made, are protected, since the person faces, dials, or addresses another person and that is a behavioral manifestation that reasonably interpreted indicates that the speech is for the faced, dialed, or addressed only. Thus there is no protection for the man who sings his secrets to himself (he could have been quiet), but only to he who confides in another (he could not do so without speech). This situation would change were simple scrambling (or real encryption) commonly used in voice communications; in that case, those who did not use those technologies would not by mere fact of facing, dialing, or addressing another be manifesting a concern with their privacy. Sounds made to oneself in the privacy of

---

[10] This is not entirely obvious. The purpose of the privilege against self-incrimination is to prevent forced, false confessions, and the like. Currently, a man can be compelled to give samples of blood and urine if properly ordered to do so. The privilege against self-incrimination has been found not to hold in these cases. (*Schmerber v. California*, 384 U.S. 757 (1966)) Thoughts are not blood samples, but are "evidence of a testimonial or communicative nature" (384 U.S. at 761) as required by *Schmerber*, but the original purpose of the Fifth Amendment may or may not be found to apply. In fact, given the overwhelming evidence that our judicial system does not reliably acquit the innocent—see Daniel J. Givelber, "Meaningless Acquittals, Meaningful Convictions: Do We Reliably Acquit the Innocent?", Rutgers Law Review 49 (Summer 1997): 1317-1396—it could be argued that the purpose of the Fifth Amendment is best served by making sure no one is prosecuted who does not think the guilty thought, and for those people, it is hard to see how a full-blown trial, rather than an extended evidentiary hearing, would be necessary for a conviction. A valid and reliable thought prober would answer the objections to computer-dispensed justice that I raised elsewhere ("The Logic of Expert Judging Systems and the Rights of the Accused," AI & Society: The Journal of Human and Machine Intelligence 2 (July-September 1988): 266-269; and "Implications of a Logical Paradox for Computer-Dispensed Justice," Journal of Law and Information Science 2 (1991): 230-232), although at a very high price in human dignity, freedom, and privacy. Broad prohibiting legislation or a Constitutional Amendment prohibiting federal, state, and private non-consensual thought probes will be better than reliance on the existing criminal procedure amendments.

one's home or vehicle that cannot be heard outside absent amplification are another matter: By choosing to sing in solitude, the person makes manifest his desire not to be heard. However, excessively loud song in solitude or loud conversation in public so loses its protection.

Perspiration, cellular residue, olfacients, waste matter: All of these are detectable by chemical sensors arrayed in micro-electromechanical systems (MEMs), all are particulate matter, and all might be monitored by police from afar to gauge truthfulness[11] when being questioned by a police officer, to give one example. Position: We wear clothing, put on deodorant and antiperspirant, bathe, change undergarments regularly, and use lotions, ointments, moisturizers, and wet wipes (not to mention the good old handkerchief) to minimize any chance of these being perceived. These are behavioral manifestations that indicate without any doubt that all traces that remain are despite our efforts. Again, it makes no difference that in this regard our efforts will always be ineffective and traces always remain — the mere effort is sufficient. However, persons who go about visibly not adhering to social norms in these regards may lose this particular protection, but the burden of proof must be on the government in any case involving bodily emissions.

The upshot of all these cases is that searches that might yield the "particularized suspicion" necessary for probable cause cannot be conducted unless there is already a particularized suspicion sufficient to make the search reasonable. However, law enforcement can use techniques to locate the bodies in a building, whether for investigative, arrest, or emergency assistance purposes, using such generalized methods as the detection of heat and sound. They can also use more particular methods, methods which home in on an individual, if that individual forfeits his rights by engaging in loud conversation, failing to bathe or otherwise attend to personal hygiene, and the like. In these cases there is no behavioral manifestation that the normally protected sphere was intended to be private.

[11] This technology is not yet available; see Rosalind W. Picard, Affective Computing (MIT Press, 1997), pp. 119ff.

Additional Cases[12]

We will consider in this section privacy rights as against individuals — tort law,[13] in other words — often involving one or two characters, Bob and Alice. It is understood that whatever is a tort when committed by an individual is a violation of civil rights when committed by the government, and *vice versa*.

A) Bob's medical records are passed around between doctors and nurses while he is receiving care. Position: Although he has not consented to particular instances, he has consented to medical care and he most assuredly wants informed care. Consent has not been bypassed, and an appropriation has not occurred.

B) Alice is sunbathing naked on **her private** beach. She is photographed in this setting. Position: This is a classical violation under the original standard if the photographer was improperly on the beach. If not, it is an appropriation under our standard since Alice's usual behavior — i.e., her behavior when not on her private beach — is to walk about clothed; that behavior reasonably interpreted demonstrates that the photographer has bypassed her consent if he somehow is able to photograph her from a remote location. (Note: This is akin to the motion and pressure sensors considered above since still photography is no less an appropriation than videorecording. The technology does not matter; that is why our standard succeeds.)

C) The photographer's published photographs of Alice (see above) are republished in

---

[12] Most of the cases in this and the succeeding section were adapted from Daniel Lin and Michael C. Loui, "Taking the Byte out of Cookies: Privacy, Consent, and the Web," Computers and Society 28 (June 1998): (2)39-51.

[13] If one tries to sue for invasion of privacy based on the three traditional torts, one will find that there are exceptions, limitations, and exclusions that we do not discuss. See *Restatement (Second) of Torts* §§652A-652I. Furthermore, privacy tort law has, in many states, been replaced by statutory law with weaker protections for privacy—New York is such a state. Finally, the First Amendment has been construed to allow much invasion of privacy (as it has been construed to allow much defamation). For an egregious example of this, in which an act state law regarded as a misdemeanor was condoned, see *New York Magazine v. The Metropolitan Transportation Authority* 136 F. 3d 123 (2nd Cir. 1998), cert. denied, 119 S. Ct. 68 (1998), which the dissent found as symptomatic of "the ever-shrinking realm of individual privacy" (136 F. 3d at 134) (2nd Cir. 1998) (Cardamone, J., dissenting). Needless to say, we regard all these developments as extraneous and unfortunate. We have also lumped together "intrusion" and "appropriation" and given wider latitude to the combination than the 1977 (i.e., very late) recodification of tort law by Prosser grants. Protecting one's privacy as against individuals is, common law or no common law, very difficult both as a matter of law and as a matter of practice in America. In this regard, the United States is less advanced than most other civilized countries. Indeed, the amount of allowed invasion of privacy and defamation is one reason to question the extent to which this nation has been civilized from the free-for-all state-of-nature.

another forum. Position: An appropriation has not occurred. Rather the tort of disclosure — another of the three ways of violating privacy — has occurred with each publication. Appropriation refers only to the original taking. It is no defense of disclosure to concede that it is not also appropriation.

D) Bob is meditating in the Grand Canyon and a group of noisy tourists come upon him. Position: By choosing to meditate in public, Bob tacitly consents to being seen and approached by others. He has not observably behaved in such a way as to seclude himself. The mere practice of an activity — meditation — usually best undertaken in seclusion cannot suffice if our standard is not to beg the question or answer it subjectively. This is one case where the requirement of reasonable interpretation may frustrate someone's expectations of privacy.

E) Bob is staring at Alice and Alice acts noticeably different — in the manner we described above under motion and pressure. Position: Here, too, there is an appropriation, particularly if circumstances prevent Alice from moving or Alice moves and Bob follows, but as with the preceding case any judgment will likely be nominal. (Note: Some readers may not be persuaded of this. Switch "Bob" and "Alice" in the story and the result will likely be more evident. Remember that we are interested in this paper only in what is objective, and not in ideology.)

F) Bob is interested in Alice, but wants to know if she's as bright as she seems. The college they both attend keeps an on-line system for academic records keyed by date of birth and mother's maiden name. Bob knows these data from Alice and keys them into the computer which shows him Alice's transcript. Position: An appropriation has occurred since the password system is an objective behavioral manifestation of concern for privacy that had to be bypassed. Curiously, although it is the college that set up the password system, since in this matter it is an agent or contractor of Alice's with the usual fiduciary responsibilities those positions of trust entail, it is Alice's privacy that has been violated.

G) A Web site sends out cookies to all who visit the site so that on their return the site can be customized to their interests and preferences, something that might sound harmless. Position: Cookies, and not Web-browsers alert to them, must ask permission to be set, no matter what their intentions, scope, etc. Nothing can be deposited on one's machine without the owner's consent. What could be plainer?[14] In fact, a cookie is a "bug," albeit an often benign bug: What could possibly give

[14] What is not plain is that an accessible Web page is not akin to someone else's private real property and just as you may be bombarded by surveillance when you enter a private physical domain—and generally have no basis for complaint—why not when the domain is virtual? The key consideration is that the cookie must disappear from memory or the C:\ drive when you are totally out of the domain, and the raison d'être of cookies (with some exceptions) is to be there when you next visit the site, thus precluding such transience.

anyone the idea that simply because someone communicates with him, he can place a bug on the line for future reference? Clearly, cookies are simply a technological development that is not yet understood.

Aggregation

A) Bob's business competitors and intimate friends can obtain from a commercial service a data image detailing his tax and credit records, his culinary preferences, and his purchasing habits. Let us assume, arguendo, that none of the components has been appropriated wrongfully: His tax returns he released when running for the school board, his credit records he released when he bought a house, his culinary preferences he gives freely to his waiter upon ordering and his grocer upon shopping, and his purchasing habits he gives to his credit-card company each time he charges an item. Position: In this case the question is centralization. But what is centralization? It is disclosure, not appropriation. It is the municipal government, mortgage-holder, waiter, grocer, and credit-card company each wrongfully disclosing, probably for a good and valuable consideration, their piece of the puzzle to the third party. However, not only can the various information providers be called to account for disclosure, the commercial service that aggregates the data can be called to account both for (further) disclosure and for presenting him in a false light. No one thing about Bob is likely to present him in a false light. However, an aggregation of particulars which presents a good slice — but not all — of the data is very likely to misrepresent Bob to a substantial degree, so while Bob will ordinarily only be entitled to a nominal award for the original disclosures (based on actual damages), the (disclosure of the) aggregation paints a picture of Bob that is deeply misleading, because it is much more than one-sided yet does not even begin to capture what makes Bob, Bob, or say what Bob is about — while, in effect, representing to say just that. Hence, a suit at law against the discloser of the aggregated information and against the aggregator of the information might well result in enormous damages even though the release of no one detail in the picture is itself damaging. In summary, aggregating data about Bob is a form of invasion of privacy[15] and its release is another, even when appropriation is not at issue.

---

[15] As against private persons, the Constitution places no such bar on law enforcement. If the aggregate picture that law enforcement creates to solve a crime is a partial and therefore substantially false presentation, the protection is that the government will bear the burden of proof at trial, and a heavy burden. Likewise such aggregation is permitted for the purposes of civil suits: Parties and witnesses are immune from defamation and invasion of privacy claims for their pleadings and testimony during the legal process (*Restatement (Second) of Torts* §§587-588). That is as it must be: We must allow fact-finding which creates a composite picture if someone has stated a sufficiently substantiated, legally cognizable cause of action and a claim for damages.

B) All of Bob's family and friends record what they see about him through their own home windows. Later, they get together and both share and compare notes. Position: This is a low-tech analogue of the preceding case.