Legal Impediments to Surveillance for Biological Threats and Countering Terrorism

Victoria Sutton, Ph.D., J.D.
Professor of Law
Texas Tech University School of Law
1802 Hartford
Mail Stop 0004
Lubbock, TX 79409
806-742-3990 x264
806-742-0251 fax
vickie.sutton@ttu.edu

ABSTRACT

The law observes jurisdictional boundaries as well as national and state boundaries, unlike biological agents. The threat of biological agents cannot be successfully controlled through surveillance technologies without removing the current impediments to a national public health approach. Public health law, traditionally and constitutionally a reserved power of the states, leaves our national defense as a combination of fifty, independently administered spheres of activity, designed by each state. However, the U.S. Constitution through a reading of The Federalist Papers, opens the door to a Congressional solution. The lack of coordination at the national level, coupled with the federalism issues has left us with no system at all.

Surveillance in the Context of Biological Threats

Surveillance by definition is "oversight, superintendence, supervision."[1] The origin of surveillance is French, and was introduced into the English language during the Napoleonic Wars period and meant "a close watch or guard kept over a person."[2] "Public Health Surveillance" is defined as "The public health practice of continual watchfulness over the distribution and trends of risk factors, injury, and disease in the population through the systematic collection, analysis, and interpretation of selected health data for use in the planning, implementation, and evaluation of public health practice."[3]

Surveillance, therefore, by definition is a continual, systematic collection of health data, necessarily collected from individuals. Constitutional protections against unwarranted surveillance include the protection of the right of privacy [4] and the protection against unreasonable searches and seizures. Surveillance may be in the form of non-invasive information collection, such as from a medical history or invasive, such as the collection of tissue samples.

State Powers v. Federal Powers for Implementation of Surveillance Systems for Biological Threats

States have police powers

State government has police powers, which are not possessed by the federal government. The Tenth Amendment provides that "powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively . . ."[5] The states are still subject to the requirements of the Fourth Amendment search and seizure requirements to obtain warrants based upon probable cause. Any other searches and seizures are unconstitutional. However, the needs of the state to protect public health have evolved a "special needs" exception in the law, which allows for a broader authority for states to conduct surveillance and public health sampling.

State governments must also recognize the constitutional right of informational privacy, through incorporation to the states of the Fourteenth Amendment.[6] Therefore, the privacy of individuals and the unauthorized disclosure of that information must be protected by the states. Information unnecessary to the narrow purpose of the state must also be avoided in the collection.

Federal government surveillance systems

Several problems exist with a federal system. Public health law is a state police power, and cannot be encroached by the federal government under the Constitution.[7] Surveillance requiring the equivalent of a "search or seizure" will require probable cause, unlike the state's exemption of "special needs" under the Fourth Amendment. Further, the right of privacy might find the fifty states information collected under 50 sets of conflicting privacy and disclosure standards.

The federal government has no coordinated surveillance system for bioterrorism or any general epidemic.[8] The national system, is instead conducted through the voluntary efforts of three national organizations: the Council of State and Territorial Epidemiologists (CSTE); the Association of State and Territorial Health Officers (ASTHO); and the Association of Public Health Directors (APHL). The Centers for Disease Control and Prevention (CDC) develops guidance for public health departments to assist in the states' efforts.

In November 2001, the CDC released a smallpox response plan, with detailed steps for local and state governments. The plan recognizes the jurisdictional limitations of state activities; for example, the plan states that "The State Epidemiologist or his/her designee *should* coordinate the epidemiological investigation in collaboration with federal health authorities. . ."[emphasis added].[9] Yet in the same paragraph, the directive is for both state and federal personnel to coordinate the investigation, and the directive has changed from "should" to "will": "The lead state *and* federal staff *will* coordinate all aspects of the investigation . . ."[emphasis added]. [10] The plan recognizes that each state jurisdiction has its own public health laws, yet states that "Although the specific mechanisms and logistics for active surveillance may differ among jurisdictional areas, the following general guidelines should be followed. . ."[11] creating a new set of guidelines for a state which in one phrase, shifts the federalism balance of control of public health law to the federal government.

The smallpox plan also recognizes the federal role of CDC as the coordinator among the states, where the activity must have a "substantial affect on interstate commerce"[12] thereby giving the federal government Constitutional authority to control this sphere of activity. For example, the guidelines specify that "If out-of-state contacts or places of travel are identified, give the information to the **CDC Coordinating Group**."[13] The state has no requirement to notify other states — although they are not prohibited from doing so — the guidance gives that responsibility appropriately to the CDC.

There are further federalism conflicts which arise in this guidance, for example, where the responsibility for tracing and interviewing persons who have had contact with a smallpox case, the guidance is unclear as to which governmental entity would designate the coordinator: "A single person should be designated by the State Medical Officer *or* Federal health authorities to coordinate tracing, interviewing, arranging for vaccination and the surveillance of contacts." [emphasis added][14]

Two national surveillance systems have been developed for specific pathogens. The National Salmonella Surveillance System, became an electronic data base in 1990,[15] and PulseNet, U.S. FDA and USDA food safety labs with four state testing labs in Massachusetts, Minnesota, Washington, and Texas, initiated in 1996. This system monitors for specific pathogens: *listeria* and *e.coli*.[16]

International systems of surveillance

Pathogens have no respect for jurisdictional boundaries, and the ease of international travel makes the threat of the spread of pathogens a likelihood. The United States has partnerships with three systems, with other world regions. The Pan American Health Organization of 21 member countries has established the Caribbean Epidemiology Center (CAREC);[17] INSPEAR, an international Network for the Study and Prevention of Emerging Antimicrobial Resistance started in 1998;[18] and PulseNet, became international in 1999-2000, when 6 provincial Canadian labs joined through their National Laboratory for Enteric Pathogens, Canadian Science Center for Human & Animal Health, Manitoba, Canada.[19]

Technologies and the Application of Law to Their Use

Public agencies' systems of surveillance

A number of systems contemplated for use by the federal government include systems which are noninvasive, as well as systems which require biological information from samples or scans of the individual. Two types of public health surveillance may include the collection of information and biological samples, as well as the systematic tracking of individuals' movements and behaviors.

The following is a list of some of the systems proposed for use by the federal government.

The BodySearch, a radiological scan of an individual, which shows the outline and details of the body, is suggested for nonmetallic searches. Some authors have proposed that the "possibility of discovering biological agents may justify the increased use of this technology in some instances,"[20] but with some level of reasonable suspicion. However, the risks associated with this technology, in exposing individuals to radiation, suggests that the risk would be weighed against the level of suspicion.

Another technology, Viisage, has been developed for facial structure recognition. The scan of faces at various angles, unlike a criminal photo identification, has created considerable difficulties in establishing reliable technology. The collection of this information would likely be challenged as a "search and seizure" without "probable cause", but the observation of a face would more likely fall under the "plain view" doctrine. The plain view doctrine holds that the faces "are in plain view,"[21] therefore there should be no expectation of privacy from the individual that someone could not see their face.

Fingerprint scans, retina scans, iris scans, voices and facial heat are other sources of unique biological characteristics which are being developed for types of surveillance systems,[22] which provide identification of the individual through these unique biological characteristics. The pattern recognition serves as the unique individual identification card. Unlike the facial recognition technology, which operates in a non-invasive way without the individual's knowledge, these scans require taking detailed information from the individual, and would very likely be considered a "search and seizure" under the Fourth Amendment.

Another system, "Bio-Surveillance" would provide surveillance for large patient populations, and is intended to provide early warning of biological and chemical attacks.[23] This system is intended to collect information from public health care providers and return to these providers any indication of a biological or chemical attack. This information is collected from existing patients, and would be protected only by the security of the computer network.

"Carnivore", a new computer surveillance system, monitors transmissions over the internet, including e-mail, sent from and to a particular IP address. There are three versions of Carnivore which operates at various levels of information: (1) the Pen Version/email only identifies the email addresses for which the individual receives or sends email messages, but not the contents of the messages; (2) the Pen Version/Web Browsing version records the internet sites visited by the individual; and (3) the Full Collection version, includes all of the functions of the other two versions, but in addition, collects the contents of the emails.[24] All versions of Carnivore are implemented by law enforcement personnel with the requirement of a warrant, which has been criticized because of the invasion of the home without "probable cause" for a "search or seizure," while a wiretap would require the obtaining of warrant.[25]

Toll booths transponders, are issued to travelers who use toll roads, and their passage through the toll booth is noted in a monthly report, which identifies the time and date of the passage through the toll booth, as well as the charge to the individual's credit card. The database can provide movements and location, date and time of vehicle through the toll booth, providing another means of private information, unless, and are typically operated by or controlled by a governmental authority, who is bound by the requirement for Fourth Amendment protections against search and seizures. Here, the character of the plain view of the vehicle is something for which the individual would have no expectation of privacy.

In 2001, however, the U.S. Supreme Court decided that sense-enhancing technology, that "was not available to the general public" would not be constitutionally acceptable for a warrantless search. In *Kyllo*, the court held that the infrared heat detection unit used which sensed the heat coming from a building in which the defendant was cultivating marijuana, constituted an illegal search without a warrant. While sense-enhancing technology was not prohibited, the court held that information that could only be obtained otherwise through a physical invasion of the premises, would not be constitutional without a warrant. This raises some questions about the use of these technologies under the current test for a warrantless search. Had *Kyllo* come before the U.S. Supreme Court after September 11, 2001, it might very well have been decided differently, and the warrantless search would have been found constitutional, because the defendant should have held no expectation of privacy for the heat leaving his building.

Private systems

Private systems and surveillance activities for the collection of health and biological information include insurance companies, private physicians and drug stores. Other types of information which might be indicative of health or personal activities affecting health are loyalty cards issued by grocery store chains and the transponders issued to drivers using tollbooth routes. Internet browsing is also an area where marketers are avidly collecting the interests and behaviors about consumers in large data bases.

Insurance companies collect health information, but most states have enacted privacy laws and requirements for insurance companies within their state. Private physicians collect private information, and have state licensing requirements as part of the protection for privacy for individuals. While, drug stores also collect information and keep records for individuals and their prescriptions, they do so with some disclosure protections. Actions for violation of privacy would range from administrative complaints for licensure, as well as common law claims of negligence or malpractice.

The loyalty cards for grocery stores operate to track the purchases of individuals who are issued the cards. Shoppers are inclined to sign up for the cards because of the discount on many products which can only be obtained through use of the card at the point of payment. Given that at least one source reports that 75% of all U.S. households have been issued loyalty cards,[26] and that 7 of the top 10 American grocery

companies offer them, [27] the ability to track behavior and purchases of specific products, as well as the time and location of such purchases, the loyalty card may enable the construction of one of the most comprehensive databases of the American public, just short of individual federal income tax reporting and social security filings.

Internet browsing information is collected by internet providers and sold to marketers, providing vast amounts of data about the behaviors, interests and other personal information about individuals. These systems are not subject to privacy rights protected by the Constitution.

Surveillance for Bioterrorism — Legal Issues

Constitutional right of privacy

The right to informational privacy is a well established doctrine[28] One of the first cases to establish this fundamental right was *Whalen v. Roe*,[29] incorporated a balancing test of privacy weighed against the governmental interest. The case, *United States v. Westinghouse Electric Corp.*[30] set out criteria for this balancing test, which are summarized as follows: (1) type of record and information; (2) potential harm of unauthorized disclosure; (3) injury as a result of the disclosure; (4) adequacy of safeguards; and (5) degree of need for access for the public interest. The Constitutional analysis requires that the governmental interest must outweigh the private interest in order for the data collection to be found constitutional.

In balancing the interest of national security against individual privacy, the national security interest will be weighed heavily in a time such as the present, when the United States is under constant alert for domestic terrorism. State law, enacted in the interest of national security will likely be upheld by the courts, where the governmental interest is exceptionally high.

Privately held and collected information; however, is not protected by Constitution. Actions by individuals are not protected by the Fourth Amendment or the constitutional right of privacy, except to the extent that states regulate professionals, hospitals and insurance companies through licenses.[31] These laws are not well defined, and vary from state to state.

Fourth Amendment

The protection from unreasonable searches and seizures[32] requires in criminal surveillance, i.e., search and seizure, that "probable cause"[33] be found.

Searches in public health law have recognized a "special needs" exception for states: "special needs beyond the normal need for law enforcement," warrant and probable cause requirement may not be applicable.[34] Compulsory screening requires limitations where persons must be "suspected" of having an infection or where persons must be "exposed" to bloodborn infections, before they may have samples taken.[35]

The critical zone doctrine, has extended the ability for government to take blood samples where the person is in the critical zone of the event. In establishing that doctrine, the court stated that "Society's judgment [is] that blood tests do not constitute an unduly extensive imposition on an individual's privacy and bodily integrity."[36]

The critical zone is another exception to the unreasonable search and seizure protection. Where the subject is in a critical zone, for example on our international borders or in the airports as an airline

passenger, the need for searches is much broader, and less protections are afforded to individuals.[37]

The critical zone doctrine might also be extended to the areas surrounding a smallpox case, for example. Critical zone analysis is not required for the surveillance of those who are "suspected" and those who have been "exposed." But in the CDC smallpox plan, which takes a concentric circle approach to the treatment of the contacts, in the outer circle, there are contacts designated as "presumptive contacts"[38] which include no known contact or exposure.

National security as a governmental interest, and the risk of biological terrorism will alter the balancing test against that of the private information interest.

In the case of emergency searches, the need for immediacy has been suggested as a basis for upholding a search without a warrant. These searches may be upheld where there are exigent circumstances and the common law doctrine of necessity.[39]

A recent concern has arisen which requires compulsory screening and surveillance of citizens who receive xenotransplantations. The risk of xenotransplantation is that viruses will be transmitted or changed when organs are transplanted from animals to humans. The need for surveillance and testing is imperative to avoid a public health risk of epidemics. The proposal for this protection would require compulsory screening and behavior modification which should be monitored under a surveillance scheme, with no "opt-out" provision. But because the risk is unquantifiable yet undeniable to the public health, insufficient basis for public health law to compel screening may exist as long as the patients are asymptomatic.[40]

The CDC smallpox plan states that it is "based on the same approach that was used to successfully eradicate smallpox more than 20 years ago and is still the most efficient approach today."[41] But the successful eradication of smallpox ultimately required the visitation of some 1200 homes in Africa in 1972, as a result of a trend in hiding smallpox cases.[42] The entry of homes where there is no "probable cause" of exposure or infection, would present a Fourth Amendment barrier in the United States.

Conclusion

In conclusion, the rights of individuals will be balanced against the unique special needs of the protection of public health. As one court aptly put the balance of individual rights, "While the constitution protects against invasions of individual rights, it is not a suicide pact."[43] The corollary to that is the statement attributed to Benjamin Franklin, "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." However, in this context, we are bargaining for more than "a little temporary safety" in the protection of the public health from potentially devastating biological attacks.

The acceptance of intrusions on individual liberties, in the context of the threat of biological terrorism, will weigh heavily in the balance of the governmental interest against the privacy interests of individuals. Those particularly concerned with privacy rights have even conceded that "We are now approaching a time when we will live in a surveillance society where all our movements and actions will be monitored."[44]

The role that the federal government has in times of war, was described by James Madison that the federal government is best to govern during "times of war" and state government is best in "times of

peace."[45] Surveillance presents another problem in the war against bioterrorism, and that is the activity must continue even in times of peace. In speaking to the reasons for keeping military in "a season of tranquility,"[46] Alexander Hamilton wrote "[W]hat time shall be requisite to ascertain the violation? Shall it be a week, a month, or a year? Or shall we say they may be continued as long as the danger which occasioned their being raised continues?"[47] Surveillance, as a peacetime activity, as well as an activity during a period of threat, such as now, could constitutionally be maintained through a federal system as forseen by the Framers of the Constitution.[48]

ENDNOTES

1. *People v. Howard*, 120 Cal. App. 45, 8 P.2d 176, 179. *Black's Law Dictionary* 4th rev'd (1968).

2. *See* Lawrence O. Gostin, *Public Health Law, Power, Duty, Restraint*, quoting The Oxford English Dictionary 309, vol. XVII (2d ed. 1989)(General Becker was the officer who was charged with the surveillance of Bonaparte).

3. Lawrence O. Gostin, et. al., *The Public Health Information Infrastructure: A National Review of the Law on Health Information Privacy*, 275 JAMA 1921, 1922 (1996).

4. U.S. Const., Amend. V.

5. U.S. Const., Amend. X.

6. U.S. Const., Amend. XIV.

7. U.S. Const., Amend. X.

8. *See generally,* Victoria Sutton, "A Precarious 'Hot Zone' — The President's Plan to Combat Bioterrorism," 164 Mil. L. Rev. 135-154 (June 2000).

9. Centers for Disease Control and Prevention, "Smallpox Response Plan, Guide A — Surveillance, Contact racing and Epidemiological Investigation," A-5 (November 21, 2001).

10. Centers for Disease Control and Prevention, "Smallpox Response Plan, Guide A — Surveillance, Contact racing and Epidemiological Investigation," A-5 (November 21, 2001).

11. Centers for Disease Control and Prevention, "Smallpox Response Plan, Guide A — Surveillance, Contact racing and Epidemiological Investigation," A-8 (November 21, 2001).

12. *United States v. Lopez*, 514 U.S. 549 (1995).

13. Centers for Disease Control and Prevention, "Smallpox Response Plan, Guide A — Surveillance, Contact racing and Epidemiological Investigation," A-16 (November 21, 2001).

14. Centers for Disease Control and Prevention, "Smallpox Response Plan, Guide A — Surveillance, Contact racing and Epidemiological Investigation," A-17 (November 21, 2001).

15. Nancy H. Bean, Stanley M. Martin, "Implementing a Network for Electronic Surveillance Reporting From Public Reference Laboratories: An International Perspective," 7 Emerg. Infect. Dis. (2001).

16. Bala Swaminathan, Timothy J. Barrett, et. al., "The Molecular Subtyping Network for Foodborne Bacterial Disease Surveillance in the United States," 7 Emerg. Infect. Dis. (2001).

17. Nancy H. Bean, Stanley M. Martin, "Implementing a Network for Electronic Surveillance Reporting From Public Reference Laboratories: An International Perspective," 7 Emerg. Infect. Dis. (2001).

18. Herve M. Richet, Jasmine Mohammed, "Building Communication Networks: International Network for the Study an Prevention of Emerging Antimicrobial Resistance (INSPEAR)," 7 Emerg. Infect. Dis. (2001).

19. Bala Swaminathan, Timothy J. Barrett, et. al., "The Molecular Subtyping Network for Foodborne Bacterial Disease Surveillance in the United States," 7 Emerg. Infect. Dis. (2001).

20. Addie S. Ries, "America's Anti-hijacking Campaign — Will It Conform to Our Constitution?" 3 N.C. J.L. & Tech. 123 at 136 (Fall 2001).

21. *California v. Ciraolo,* 476 U.S. 207 at 212 (1986). *See also* Addie S. Ries, "America's Anti-hijacking Campaign — Will It Conform to Our Constitution?" 3 N.C. J.L. & Tech. 123 at 142-43 (Fall 2001).

22. Eric Slater, "Not Everyone Sees Eye to Eye on Biometrics," *News and Record* (Greensboro, NC), p.D2 (Friday , June 12, 1998).

23. "MC Strategies Announces Surveillance System to Provide Early Warning of Biological or Chemical Incident," *PR Newswire*, Financial News (Tuesday, November 13, 2001).

24. Harold Lewis, David Lange, Robert Cottrol, David Steinberg, "Privacy on the Internet," Panel Presentation, American Association of Law Schools Annual Meeting, New Orleans, LA (Sunday, January 6, 2002).

25. *Id.*

26. Katie Fairbank, "Grocery shoppers sick of being carded; many resent trading information for savings; stores tout benefits," 1A *The Dallas Morning News* 2d ed. (Wednesday, Dec. 19, 2001).

27. Jennifer Hoyt, "Savings cards offend privacy advocates," B08 *The Deseret News* (Monday, January 28, 2002).

28. Lawrence O. Gostin, *Public Health Law, Power, Duty, Restraint* 132 (2000).

29. 429 U.S. 589 (1977).

30. 638 F.2d 570, 578 (3d Cir. 1980)

31. Lawrence O. Gostin, *Public Health Law, Power, Duty, Restraint* 132 (2000).

32. U.S. Const., Amend IV.

33. U.S. Const., Amend IV.

34. *Schmerber v. California*, 384 U.S. 757, 767-68 (1966).

35. Lawrence O. Gostin, *Public Health Law, Power, Duty, Restraint* 193 (2000).

36. *Skinner v. Railway Labor Executives Ass'n*, 489 U;.S. 602 at 625 (1989) (Upholding drug tests following accident even without reasonable suspicion of impairment.) *See also*, Addie S. Ries,

"America's Anti-hijacking Campaign — Will It Conform to Our Constitution?" footnote 14 N.C. J.L. & Tech. 123 (Fall 2001).

37. *See* Addie S. Ries, "America's Anti-hijacking Campaign — Will It Conform to Our Constitution?" 3 N.C. J.L. & Tech. 123 (Fall 2001).

38. Centers for Disease Control and Prevention, "Smallpox Response Plan, Guide A — Surveillance, Contact racing and Epidemiological Investigation," A-17 (November 21, 2001).

39. A. L. DeWitt, "The Ultimate Exigent Circumstance, 5 Kan. J.L. Pub. Pol'y 169, 173-75 (1996)(justifying FBI activity).

40. Patrik S. Florencio and Erik D. Ramanathan, "Are Xenotransplantation Safeguards Legally Viable?" 16 Berkeley Tech. L.J. 937, 958-59 (Summer 2001).

41. Centers for Disease Control and Prevention, "Smallpox Emergency Preparedness and Response Information, Questions and Answers," Draft –for internal use only (November 23, 2001).

42. Interview with Stanley O. Foster, M.D., by Harry Goldhagen, "Talking About Bioterrorism. Smallpox: The Weapon That Knows No Borders," 3 *Medscape Infectious Diseases* (2001). Website visited Feb. 14, 2001 http://www.medscape.com/viewarticle/414954. (Dr. Foster was a key player in the battle against smallpox in Bangladesh, Nigeria and Somalia during the 1960s and 1970s.)

43. *Kennedy v. Mendoza-Martinez*, 372 U.S. 144, 159-60 (1963).

44. Quotation from Barry Steinhardt, ACLU, Laurie Belsie, "Slide Toward Surveillance Society, The Christian Science Monitor, at 1 (Feb. 26, 1999).

45. The Federalist No. 45 (James Madison)(Clifford Rossiter ed. 1961).

46. The Federalist No. 25, 164-65 (Alexander Hamilton)(Clifford Rossiter ed. 1961).

47. *Id.*

48. *See generally,* Victoria Sutton, "Bioterrorism Preparation and Response Legislation — The Struggle to Protect States' Sovereignty While Preserving National Security," 6 *The Georgetown Public Policy Review* 92-103 (2001).