A Framework for Comparing Perspectives on Privacy and Pervasive Technologies

Developing a framework for judging pervasive technologies against social norms can give technology developers insight into how and why the systems they create test those norms.

Anne R. Jacobs and Gregory D. Abowd
Georgia Institute of Technology

Each of the many viable definitions of personal privacy reflects a distinct set of beliefs about what types of information the courts should protect.[1] As those beliefs change and evolve, so does the law. Pervasive computing research has also evolved, investigating mechanisms for supporting some predefined notion of privacy, typically favoring individual rights over the rights of the community. We offer a framework to consider individual and group rights so that technology developers can more effectively reason about concerns for existing technology as well as generate new technologies that respect a well-defined set of social norms.

No matter what the technological solution, multiple viewpoints will likely conflict on the merits of that solution. Much of the work of the law is devoted toward resolving these types of struggles between competing claims over rights. Therefore, we looked to the legal community for insight into ways of handling this kind of conflict. This article outlines a framework designed to help developers understand the conflict between privacy and pervasive computing technologies, particularly those technologies that deal with sensing and storage. Pervasive computing technologies, especially those that can automate perception of human activity and then store that information, can provide tremendous benefits. However, they generally require access to information about an individual's identity, location, and activities that often challenge definitions of personal privacy.

Consequently, these emerging technologies have forced us to ask a very important question: What are the implications of these challenges for the meanings that we, as a society, want to assign to personal privacy and for the legal protections that we want to give to it? We offer an analytic method to assist developers in asking these questions about the systems and applications they are creating. We believe this framework will help developers minimize the gap between design goals and actual effects on privacy.

Privacy and pervasive computing

Legal challenges to pervasive computing systems have largely centered on the question of whether using certain systems constitutes a search according to the Fourth Amendment to the US Constitution. The sidebar "Relevant US Supreme Court Decisions" summarizes several key cases relating to privacy and technology, including *Katz v. United States* (1967), *Kyllo v. United States* (2001), *Silverman v. United States* (1961), and *United States v. Karo* (1984). When a government agency uses a sensing system to collect data, the legal questions often entail whether that

Published by the IEEE CS and IEEE ComSoc ■ 1536-1268/03/$17.00 © 2003 IEEE

Relevant US Supreme Court Decisions

This sidebar consists of direct excerpts of the key elements of four Supreme Court decisions. You can find the full text of these decisions at www.findlaw.com/casecode/supreme.html.

United States v. Karo (1984)

"At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable. Our cases have not deviated from this basic Fourth Amendment principle. Searches and seizures inside a home without a warrant are presumptively unreasonable absent exigent circumstances. In this case, had a DEA agent thought it useful to enter the Taos residence to verify that the ether was actually in the house and had he done so surreptitiously and without a warrant, there is little doubt that he would have engaged in an unreasonable search within the meaning of the Fourth Amendment. For purposes of the Amendment, the result is the same where, without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house. … Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."

Silverman v. United States (1961)

"The instrument in question was a microphone with a spike about a foot long attached to it, together with an amplifier, a power pack, and earphones. The officers inserted the spike under a baseboard in a second-floor room of the vacant house and into a crevice extending several inches into the party wall, until the spike hit something solid 'that acted as a very good sounding board.' The record clearly indicates that the spike made contact with a heating duct serving the house occupied by the petitioners, thus converting their entire heating system into a conductor of sound. Conversations taking place on both floors of the house were audible to the officers through the earphones. [A] fair reading of the record in this case shows that the eavesdropping was accomplished by means of an unauthorized physical penetration into the premises occupied by the petitioners. Eavesdropping accomplished by means of such a physical intrusion is beyond the pale of even those decisions in which a closely divided Court has held that eavesdropping accomplished by other electronic means did not amount to an invasion of Fourth Amendment rights."

Katz v. United States (1967)

"At trial the Government was permitted, over the petitioner's objection, to introduce evidence of the petitioner's end of telephone conversations, overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls. The Government stresses the fact that the telephone booth from which the petitioner made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside. But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."

Kyllo v. United States (2001)

"Suspecting that Danny Kyllo was growing marijuana, police officers used a thermo imager to conduct a scan of the exterior walls and roof of his home. Both the officers and the imaging device were located on public property across the street from the home at the time that it was used. The imager captured the infrared radiation emanating from the exterior walls of the home and transformed that input stimulus into a black and white pattern of relative heat distribution. The results were consistent with the amount of heat produced by the type of lamp used to cultivate marijuana. Based upon an interpretation of the captured scan, along with other corroborating evidence in the shapes of informants' statements and utility records, the police were able to secure a search warrant for the interior of Kyllo's home. The Supreme Court ruled, with a slight 5-4 majority, that use of the thermo imager qualified as a Fourth Amendment search and, therefore, officers were required to have a warrant prior to performing the scan."

action constitutes a search or seizure and, if either, whether the activity is reasonable. In answering these questions, the courts look to the specific details of the incident in question.

The court assesses the details associated with the place of the incident and the action taken there to determine whether the person involved expressed a subjective expectation of privacy and whether that expectation is one that society recognizes as reasonable. The pertinent issues for technology, considered through the lens of US law, include the following: the physical nature of the input stimulus,

The European Union's Data Protection Directive

In the European Union, the Data Protection Directive is the general policy that applies to all personal data, particularly the kind of personal data that could identify a particular person. According to the DPD, the courts make exceptions for types of processing conducted for purely personal reasons, household purposes, or matters pertaining to a member country's internal concerns, such as domestic security, defense, and criminal law enforcement. Often, it might not be easy to distinguish between uses that are entirely personal and those that are not. Domains beyond the scope of the DPD are governed by each country's own laws. According to the DPD, each member state must craft its own legislation to effect the directive's terms.

The DPD focuses on several issues that parallel issues that have emerged in US courts. For example, the physical nature of the input stimulus that the sensing system detects and the granularity of the information produced are both open to question. Can a particular person be identified from either the input stimulus's physical nature or the information's granularity? The initial inquiry can help determine whether the sensing system is within the DPD's scope. Because both factors are amenable to multiple—and often contrasting—descriptions, there is much disagreement in the EU about the DPD's applicability. For example, does the stimulus alone identify a person or is it only one bit of evidence that is insufficient by itself to render positive identification?

The sensing device's location, how the system detects the input stimulus, and the location from which the input stimulus originates are all relevant. Does a member state's DPD legislation indicate that certain physical areas are ones of heightened privacy protection so that intrusion through physically placing the sensing device is prohibited or does a person have greater privacy rights in the stimuli that originate in these special areas than in stimuli that originate elsewhere? If a sensing system does not fall within the purview of the DPD, system developers might best begin their considerations of privacy implications by looking at a member state's laws relating to those domains exempted from the DPD, such as criminal law, domestic security, and defense.

the location from which the input stimulus originates, the location of the sensing device, how the system detects the input stimulus, and the granularity of the information produced. (The European Union is dealing with similar issues. See the sidebar "The European Union's Data Protection Directive.")

The physical nature of the input stimulus can determine the presence, or absence, of a recognized privacy interest. Does an individual have a privacy interest in some types of stimuli but not in others? In *Katz v. United States*, the court held that an individual has a privacy interest in the sound waves produced by speech. Similarly, the majority opinion in *Kyllo v. United States* found a privacy interest in the thermal radiation that is emitted from the interior of a home. In addition, does the stimulus originate in a public place (such as a store) or in a private place (such as a home)? The court recognizes privacy interests as being much stronger for objects placed in sheltered areas than those that are placed in public view. The privacy implications of a sensing system that detects input originating in an area of heightened protection are considerably greater than for one that accepts input from a public area.

The courts have also determined that some physical spaces have greater expectations of privacy associated with them than do others. The simple presence of a sensing device within an area of heightened expectations might constitute a privacy violation. This fact was the cornerstone of the decision rendered in *Silverman v. United States*. The mechanism by which the system detects the input stimulus is also very important. Whether a sensor waits passively to be struck by stimuli in the public domain or sends out an excitation signal that might cross into a private space can determine whether the courts will recognize a privacy interest. This distinction was of great importance to the dissent in *Kyllo v. United States*.

The granularity of the information produced can also be a key factor in court decisions. Does the information provide details about what is occurring in a private place or does it merely provide a basis from which an inference can be drawn about what is occurring? The majority and the dissent in *Kyllo v. United States* arrived at opposite answers to this question. The majority found that the information did provide details about activities inside the home, whereas the dissent said that the information did no more than help to establish a basis from which inferences could be made.

Analytic framework

Examining the combination of hardware, software, and use factors raised by these issues can help determine an action's legal status. For purposes of the Fourth Amendment, the legal status determines whether the government's actions fall within the scope of subjective expectations about privacy that society recognizes as reasonable. However, the process of determining an action's status is often more complex than it first seems to be. Even when two people look at the same system design and its application, they might evaluate the privacy effects in entirely different ways. As happened in several key privacy cases, courts might describe the same factors differently and even assign different relative weights to those factors.

TABLE 1

Terrell's four-box representation of different perspectives for reasoning about a technology's social implications.

Box 1	Box 2
Audience: Community **Reasoning:** Rights-based **Summary:** All people must respect one another's autonomy. The government must also protect individuals' rights.	**Audience:** Political **Reasoning:** Rights-based **Summary:** All individuals belong to a community. Behavior that supports the community is highly valued. Although ties between community members are legitimate, individuals remain more important than any specific social objective. Therefore, the government cannot adopt policies that, in valuing the group, disregard the rights of the individual.
Box 3	**Box 4**
Audience: Community **Reasoning:** Goals-based **Summary:** Supporting autonomy at the community level is more important than encouraging connections between individuals. National policy, to the contrary, is focused on the society's own sense of its character and long-term destiny.	**Audience:** Political **Reasoning:** Goals-based **Summary:** Each person should behave in ways that foster community strength. The government's core purpose is to support small communities through appropriate policies at the societal level. The goal of improving society justifies the possible negative consequences to individuals.

We base our analytic framework on work first done in the field of legal ethics by Timothy P. Terrell. Terrell's model is rooted in metaethics, an area of philosophy that deals with the ways in which values are expressed rather than with the content of the values themselves.[2] Terrell uses four categories: The first two pertain to scale and the second two to assessment. Scale describes the size of the group toward which an argument or a policy is directed. For example, when the audience is large, the level becomes political and the concerns address social institutions and justice. When the audience is small, the level moves to the community where the questions entail how individuals should treat one another.

Terrell's assessment criteria focus on the standards used to evaluate behavior. A rights-based perspective holds that there is a set of values that mark actions as either acceptable or unacceptable. In contrast, a goal-directed perspective would judge an action according to its contribution toward the realization of a particular objective. The arguments and policies that an individual advocates are comprised of both scope (political or community) and the reasoning style (rights-oriented or goal-oriented). As Table 1 shows, the combination of these elements yields a four-part box that represents the range of perspectives from which we can analyze just about any social or policy issue. This structure occupies a principal place in philosophical analysis.[3,4]

Where other legal and philosophical scholars use the four-part box model to ground prescriptive arguments,[5,6] Terrell employs the boxes for descriptive purposes. By analyzing the reasoning behind their beliefs, Terrell seeks to understand why people disagree about the correct legal response to morally and legally ambiguous situations. In Terrell's application of the boxes, the boundaries between the quadrants are porous. Instead of being impenetrable walls, the boundaries between the areas become markers on a long, continuous spectrum. Depending on the particular issues being considered, the same person will likely occupy different positions on the spectrum. We do not intend to imply that one box is better than another or that there is a desired progression from any one of the boxes to any of the others. The purpose of the boxes is to enrich understanding of the diverse perspectives that people bring to their beliefs about privacy rights.

Using the framework

Having defined our framework for distinguishing different perspectives, we will briefly explain how to apply it. Our first example, a post hoc explanation of differences in opinion in the case of *Kyllo v. United States*, demonstrates how concrete facts can still be interpreted in different ways. The majority and dissenting opinions in this case provide a clear example of how the characteristics of the hardware and software factors, in conjunction with the different options for audience size and reasoning style, can lead to different legal conclusions. An extended analysis of this case—using the four-box framework—can be found elsewhere.[7]

Majority opinion

The majority opinion, authored by Justice Scalia, approached the case from the Box 1 perspective of the individual (the smallest sense of a community) and used a rights-based reasoning style. The court applied the rule that the individual's right to privacy within the home outweighed any consideration of benefits that might accrue to the larger surrounding society. The majority considered each of the factors from the position of the detached individual looking outward rather than from the position of the larger society looking inward. The court's definitions of each component reflected what will best support the individual's rights. Together, these components led to the

court's conclusion that using the thermo imager without a warrant violated homeowner Kyllo's privacy interests.

The court said that the black and white pattern of heat distribution that rose from the home was "information regarding the interior of the home and not merely information about the home." Conflating the input stimulus and the information produced, the court equated the thermal radiation input with the audio waves produced by a human voice. Not mentioned in the case ruling is the fact that the latter could be reverse-engineered to yield the exact words spoken, whereas the former cannot be processed to reveal the precise temperatures. This omission let the court extend the privacy interest previously found in the content of confidential conversation to temperature levels.

The majority did not contest that the thermo imager was located on public property when the police conducted the scan and that it did not emit any type of rays or beams. However, the sum of the extent of emphasis on the granularity of the information produced (including affirmation of a privacy interest in the input stimulus), a rights-based reasoning style, and an almost exclusive focus on individual rights, induced the court to dismiss the passive nature and public location factors.

Minority opinion

The dissent, authored by Justice Stevens, emerged from a Box 3 perspective. The goal of Box 3 is to balance rights and responsibilities pertaining to information that is in the public domain with rights and responsibilities associated with information that is in the private arena. The minority's finding indicated that national interests in the social benefits that are possible only with easy access to information should be tempered by sincere respect for the rights of the individual to privacy within his or her home.

The minority's characterization of the hardware-software factors at issue demonstrates the opinion's roots in Box 3. The minority argued that an individual's rights, while always important, must be balanced with the interests of the populace as a whole. The thermo imager passively received the stimulus (heat energy) emitted from the exterior walls of Kyllo's home. The dissent's findings that the stimulus did not originate inside of the home and that the thermo imager did not physically penetrate the boundaries of the home (via emissions of any type) were key to its conclusion that no violation of privacy occurred.

In sharp contrast to the majority, the minority opinion found that the information produced was not only coarse ("relative differences in emission levels") but that it was also about the exterior, not the interior, of the home ("vaguely indicating that some areas of the roof and outside walls were warmer than others"). The majority and the minority agreed that the thermo imager was located in a public space. In the dissent, however, this element reinforces the strength of the other hardware-software factors. In the majority, the location component was eclipsed by the granularity of information and source of input stimulus factors.

Existing pervasive technologies

The courts are not the only places where these issues are relevant. Pervasive technologies raise privacy issues all around us each day. What follows are two examples based on our own experiences using an automated lecture-capturing system called eClass (formerly Classroom 2000).[8] The following scenario describes a potential use of the captured archive repository and subsequent reactions to the storage and access policy for the system. Although fictitious, the scenario represents real privacy concerns.

Injurious comments

An instructor uses eClass in a graduate seminar in which everyone discusses journal papers. The instructor openly criticizes the research method of a particular paper, implying that one of its authors consistently exhibits poor habits in his research. One of the students in the class disagrees with the instructor's assessment and contacts the author to point him to the recorded lecture. The author accesses the lecture and listens to the discussion about his work. He is upset by the tone of the instructor's comments and calls the department's chair to lodge a formal complaint. The author claims that the instructor portrayed him in a misleading light and requests that the recorded material be removed. The department chair decides that the instructor must protect the captured lecture materials with a password so that, when accessed through the official class site, the lectures are available only to students enrolled in the class.

From the perspective of Box 1, the analysis would focus on the rights of the individuals: the instructor's and students' rights to free speech, the instructor's right to protect his intellectual property, and the author's right to privacy. According to a Box 1 analysis, protecting individual rights is the rule that guides behavior at both the small group level and at the societal level. Protecting one person's rights might have adverse consequences for another person, but that is inevitable. Following this reasoning, the department chair might decide that the author's right to privacy trumps the free speech and privacy claims, believing that the value of the right to be free from false and misleading portrayal is in the benefits that it bestows on the individual. The duty of the department chair, as the leader of the department community and a member of the university administration, is to protect the rights of the individuals who make up the department

and the university. His duty exists at both the moral level of the classroom and the political level of all audiences to whom a faculty member could make the material available through university resources. The password requirement for materials on the class site is the best way, he believes, to fulfill his protective duty.

A Box 2 perspective would place the free speech and privacy interests of the individuals within a network of community values that honors and seeks to preserve connections between people. The department chair, according to a Box 2 perspective, believes that the department community's cohesiveness would best be preserved by restricting the extent to which department computing resources could be used to disseminate provocative opinions beyond those who would, in any event, have exposure to them in the classroom.

At the political level beyond the university, the department chair's approach becomes categorical. Individual rights are important by themselves and must be protected. The desire to create a certain type of community, no matter how compelling, cannot be pursued at the cost of individual's rights. Therefore, the chair invokes the same reasoning as he does in Box 1. He understands the benefits of the right to privacy as belonging primarily to the individual and the benefits of the rights to free speech and intellectual property as being in the form of progress toward a particular type of society. The chair's duty is to protect the rights of the individual at the moral level of the department and at the political level rather than to promote a given type of society.

Within the limited context of the department community, a Box 3 analysis would lead the department chair to place the emphasis on protecting the author's right to privacy for reasons outlined under Box 1. However, once beyond the department, the chair becomes a consequentialist in his reasoning. In the name of national character and destiny, the state can set a balance between individual rights and community claims. What resolution of the competing assertions of the instructor, student, and author will, without trampling any of the rights, go furthest toward protecting the national character? The chair decides that limiting the password requirement to those captured materials placed on the official class Web site is the solution.

Concern for social character and national destiny dominate the Box 4 analysis. What is the best way to foster cohesiveness within the department community? What is the best way to pursue social goals without overrunning the rights of any individuals? The department chair believes that the way to promote departmental cohesion is, as Box 2 suggests, to limit access to the captured lecture materials on the class Web site.

Right to not be recorded

Our second hypothetical scenario involves a student who objects to being recorded in an eClass setting because the idea of being recorded makes him too uncomfortable to speak in class. Upon hearing this, the instructor asks the class to indicate their feelings on this issue. All other students do not mind being recorded, so the teacher decides to keep the eClass capture going, not just because there is majority support, but because the majority is overwhelming. The lone student lodges a formal complaint with the university, claiming that recording him compromises his right to a fair educational environment.

Does a student or professor have a right to a fair educational environment? If so, is the enjoyment of that right enhanced or impaired by a system that records and archives classroom discussions? The differences in how each of the four boxes approach the relationships between the individual and the community are evident in the way that each of the boxes frames these questions. For example, in a Box 1 analysis, the focal point of both the moral and political dimensions is safeguarding the individual's rights, so the fact that the majority vote was overwhelming is irrelevant. The central question is whether a student has a personal right to a fair educational environment and, if so, how that right is defined. Only when those questions are answered can the inquiry move on to what enforcing that right means. The concern at this point—according to Box 1—is with the rights of the single student and not with the rights of the group.

Box 1 approaches the question about whether the right to a fair educational environment can be justified through the claims that an individual can make on the surrounding community. Claims that the community and state make on the individual are not germane. However, we could ask how the rights of the professor and of the individual students in favor of the recording should be weighed against those of the objecting student. What constitutes a fair educational environment for the professor and other students? Does the professor's right include selecting the technology to be employed in the classroom? The Box 1 perspective indicates that each individual must respect the rights of other individuals. How can we respect the rights of each of these three parties?

According to Box 2, it is important that the objecting student is situated within the class and the university communities. These two groups have legitimate claims upon the student. The student's exercise of rights at this moral level is constrained by those claims that are directed toward the goal of promoting interpersonal connection. How is a fair educational environment defined in this context? If that right exists, does it belong to the individual or to the com-

the AUTHORS

Anne R. Jacobs is a research assistant at the Emory University School of Law. Previously, she was a research scientist at Georgia Institute of Technology. Her research interests include the intersections between law, technology, and medicine. She received a JD and an MDiv from Emory University and an MS in human-computer interaction from the Georgia Institute of Technology. Contact her at ajacobs3@cox.net.

Gregory D. Abowd is an associate professor in the College of Computing and the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology. His research interests involve applications research in ubiquitous computing, concerning both HCI and software engineering issues. He received a D.Phil in computation from the University of Oxford. He is a member of the IEEE Computer Society and ACM. Contact him at abowd@cc.gatech.edu; www.cc.gatech.edu/fac/Gregory.Abowd.

munity as a whole? How will recognizing a right to a fair educational environment, particularly one that includes the freedom not to be recorded against one's will, affect the cohesiveness of the classroom and of the university?

At the political level, the inquiry is a bit different. The state is obligated to protect the individual's rights. It cannot impair those rights for the sake of promoting social goals, such as communal cohesiveness. As with Box 1, the quandary in Box 2 remains how to protect the rights of all the parties involved. However, in Box 3, defining and protecting the right to a fair educational environment entails focusing on the individual and not the classroom or university communities. The rights of the individual students and professors that make up these groups take precedence over the groups as a whole. The fact that the rights of a single person are asserted against the desires of an entire group does not undermine the former.

At the political level in Box 3, the disparity in numbers does become a factor. The single person is part of the social structure that speaks through the group's voice. Defining and exercising an individual right to a fair educational environment is colored by considerations about how that right will impact the classroom and university communities—in addition to the larger society. A positive effect is acceptable but a negative one is not.

In a Box 4 analysis, considerations for an individual's right to a fair educational environment must be set against the backdrop of community interests. Box 4 favors rights and expectations that are conducive to group cohesion and destiny over those that treat the individual as an isolated entity. To the extent that the overwhelming majority of students in support of the recording is evidence of what will encourage connections among members of the class, this is a point on which analysts could easily come to different conclusions. Why should the larger numbers be deemed evidence of what will promote social connections?

Legal conceptions of privacy reflect prevailing social norms. Pervasive computing technologies challenge those norms because they often access information that has long been deemed to fall within the scope of individual privacy. Designing policies that realize the full potential of pervasive technologies while simultaneously protecting privacy begins with understanding the interaction of these elements with one another. Such understanding is a critical element in deciding what we, as a society, want the new social norms to be.

The paradigm we presented here outlines two important dimensions that directly affect any determination that a developer might make in assessing the social implications of pervasive technologies: the audience of concern (society as a whole or smaller communities) and the motivation of the reasoning process (rules-based or goal-based). We hope that in discussing these dimensions in the context of pervasive technology, we can provide a valuable framework for exploring the implications that different system designs have for privacy. P

ACKNOWLEDGMENTS

We received support for this work from a National Science Foundation ITR Grant and from the Aware Home Research Initiative industrial consortium. We thank Timothy P. Terrell from the Emory University School of Law for his continued intellectual support of this work.

REFERENCES

1. R. Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort," *California Law Rev.*, vol. 77, Oct. 1989, pp. 957–1010.
2. T.P. Terrell, "Turmoil at the Normative Core of Lawyering: Uncomfortable Lessons From the 'Metaethics' of Legal Ethic," *Emory Law J.*, vol. 49, no.1, Winter 2000, pp. 87–133.
3. J. Rawls, *A Theory of Justice*, Belknap, 1972, pp. 65–75.
4. S. Fishkin, *The Dialogue of Justice*, Yale Univ. Press, 1992, pp. 50–53.
5. K. Nielsen, "Problems of Ethics," *Encyclopedia of Philosophy, vol. 3*, P. Edwards, ed., Macmillan, 1967, pp. 117–134.
6. R. Simon, "Social and Political Philosophy," *Encyclopedia of Ethics, vol. 2*, L.C. Becker, ed., Routledge, 1992, pp. 11–63.
7. T.P. Terrell and A.R. Jacobs, "Privacy, Technology, and Terrorism: Bartnicki, Kyllo, and the Normative Struggle Behind Competing Claims to Solitude and Security," *Emory Law J.*, vol. 50, no. 4, Fall 2002, pp. 1469–1511.
8. G.D. Abowd, "Classroom 2000: An Experiment with the Instrumentation of a Living Educational Environment," *IBM Systems J.*, vol. 38, no. 4, Oct. 1999, pp. 508–530.