Privacy: in the context of past, present, and emerging technologies

Chetan Jindal
Yale College 2004
May 3, 2004

Computer Science 490
Advisor: Professor Joan Feigenbaum
Privacy: in the context of past, present, and emerging technologies
Chetan Jindal
Yale College 2004, Computer Science 490
May 3, 2004

Defining Privacy
In a paper on a highly nuanced topic such as privacy, it is essential to set up a working definition at the outset. For privacy, the problem of articulating a comprehensive definition has been particularly intractable. What is privacy? What does it entail? And what does it exclude?

Determining the variables across which any definition of privacy must be valid is a possible first step. Any definition must be relevant at both the individual and group levels. It must take into consideration personal preferences, as well as socially endorsed ethical and moral standards. It must factor in governmental control over persons. It must also, perhaps most crucially, allow for some measure of flexibility necessitated by changing times (and a good measure of robustness to withstand disruptive change). This is a partial, and contestable, list of relevant privacy concerns. Robert Gellman, contributing writer to Technology and Privacy: The New Landscape, cautions us of the inevitable difficulties in formulating a universal definition of privacy, arising precisely out of this multitude of constituent variables. “There is no reason to believe that a new effort to define privacy [...] will achieve consensus,” Gellman writes quoting Alan Westin, a noted privacy scholar, “because privacy issues are fundamentally matters of values, interests, and power.” Instead, the long-standing, simple, and open-ended formulation made popular by Louis Brandeis, that privacy is “the right to be let alone,” has repeatedly emerged in privacy scholarship as a useful approximation to a precise definition.

Privacy and Technology: Historical Evidence
Famously appearing in Olmstead v. United States, 277 U.S. 438 (1928), as a part of Brandeis’ dissenting opinion, the statement serves as a historic focal point for the study of privacy in the context of technology. Briefly, the circumstances of the case were as follows: Olmstead was charged with “conspiracy to violate the Prohibition Act.” The basis of the charge was a series of incriminating telephone conversations between the plaintiff and various third parties. Evidence of these conversations was obtained by government agents through the tapping of telephone-lines running out of Olmstead’s residence. The principal points of contention in the case were whether governmental wire-tapping (performed in public spaces and without physical intrusion into the plaintiff’s dwellings) violates Fourth Amendment protections against “unreasonable searches and seizures,” and if inclusion of the recorded conversations in the proceedings “compel[s] the accused to be a witness against himself in violation of the Fifth Amendment.” The case was ruled in the government’s favor.

Quoting preceding case-law, Brandeis dissented as follows:
But “time works changes, brings into existence new conditions and purposes.” Subtler and more far-reaching means of invading privacy have become available to the Government. 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.

2 Olmstead v. United States, 277 U.S. 438, 572 (1928) (dissenting opinion).
Moreover, "in the application of a constitution, our contemplation cannot be only of what has, been but of what may be." The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may someday 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. "That places the liberty of every man in the hands of every petty officer" was said by James Otis of much lesser intrusions than these. [...] 

[The authors of the Constitution] sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone – the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth. 

In arguing against the prevailing opinion (which was delivered by then Chief Justice Taft), Brandeis was positing a theory of privacy based on first principles as enshrined in the Constitution, but also a theory valid in the larger supra-legal privacy debate. Most importantly, Brandeis was recognizing that privacy is an ever-changing open-ended issue, and that any discussion of privacy must be predicated on the current state of technology. It may not be too much of a stretch, in fact, to view the privacy debate as a reactionary off-shoot of technological evolution. Gellman captures the idea succinctly, “In many ways,” he writes, “the battle over privacy in the twentieth century has been a struggle over adapting privacy principles to constant technological advances.” In the light of this observation, it is easier to understand why it has been difficult for academic and legal scholars to propose a conclusive definition of privacy. Because if privacy analysis is predicated on technology, and if technology changes with time (as it surely does), then attempts to arrive at a static definition of privacy are doomed to failure. It remains unclear, in fact, if a terminal definition of privacy is possible at all, even only if far into the future.

Brandeis’ predictions are not off the mark. It is easy to find current technologies that present privacy challenges analogous to the ones of his time. Brandeis’ wiretapping is today’s IP traffic interception. His “instantaneous photographs” are today’s computational face-recognition programs. His “evil [...] invasion of privacy by the newspapers” is equivalent to the for-profit distribution of consumer information by today’s data profiling companies. In each case, current technologies have posed novel privacy challenges that were previously unforeseeable. And alarmingly, like wiretapping at the time of the hearing of Olmstead v. United States, these challenges are now observable but have not yet been satisfactorily dealt with.

Open Questions

What, one can ask, is different in each case that technology threatens privacy? And what, if anything, is similar? Is each new challenge posed by emerging technology fundamentally different from previous ones? If each new challenge is different, then is it at all possible to prepare for new challenges ahead of time, and before their negative effects are felt? In other

---

3 Gellman, 203.
words, is it possible to proactively tackle future privacy challenges today (in addition to tackling current and past unresolved challenges)?

**Potential Sources of Threats to Privacy**

I believe that most of the privacy challenges facing us today stem primarily from the following broad technology categories:

(A) The computational feasibility of collating large amounts of distributed data, and of searching for patterns in such data:

Data collection and mining techniques have been pioneered by commercial establishments such as ChoicePoint. The following promotional text appears on the company’s official website: “For almost a century ChoicePoint has been a trusted source and leading provider of decision-making information that helps reduce fraud and mitigate risk. ChoicePoint has grown from the nation's premier source of data to the insurance industry into the premier provider of decision-making intelligence to businesses and government. Through the identification, retrieval, storage, analysis and delivery of data, ChoicePoint serves the informational needs of businesses of all sizes, as well as federal, state and local government agencies.”

Because we now increasingly live our lives in electronic spaces, such as the internet and office intranets, and because we participate in electronic transactions, a large amount of our personal data is maintained digitally. In addition, electronic archival is accepted as a superior alternative to physical storage of personal documents. Therefore, large chunks of private data are now available in binary format, suited to easy transmission and automatic processing. Concurrently, an exponential increase in computing power has transformed the privacy landscape analogous to the way that the development of nuclear weapons changed conventional warfare. All the data about us that is available today to second parties may also have been available previously, but in the past it was infeasible to mine it effectively. Positive uses of data collation do exist, as the ChoicePoint blurb highlights, but the potential for negative use is severe.

(B) The ability to inconspicuously record certain individual actions, habits, and information:

It is now possible for second parties to discreetly record details of our interactions with them. Websites can easily log usage, indexed by IP addresses. Online merchants are able to combine usage data with the names and addresses provided by consumers during checkout. Even retailers in the real world can build purchase histories by requiring a persistent identifier (such as a store supplied shopping card) at the time of checkout.

Surveillance cameras can archive video-feeds from monitored spaces, making it impossible for individuals to anonymously use these spaces. Cameras smaller than a fingernail, capable of transmitting data over the air, can be easily camouflaged if required.

RFID tags and hidden trackers can transmit an individual’s coordinates back to controlling stations in real time. Potentially, the history of a person’s movement could be electronically stored on remote servers without his even knowing it.

Such ability for invisible monitoring has existed previously, but only in much weaker forms. The scale at, and ease with, which surveillance can now be performed poses a serious privacy threat.

(C) The ability to parse unchanging and undeniable biometric identifiers:

---

Face-recognition software can scan and match individuals against existing databases in real time. New faces can be archived, and the reappearance of old ones can be logged. Like surveillance cameras, face-recognition systems make it impossible to use monitored spaces anonymously. Other kinds of biometric information, such as finger-prints, retinal-patterns, and DNA, provide additional means of persistent, undefeatable, and ever-present identification.

The highly alarming fact about biometric identification, is that it is almost impossible to refuse a demand for biometric information. A person cannot hide from face-scanning systems (short of wearing a mask), nor can he avoid being finger-printed or retinal-scanned. The technology for unobtrusive biometric identification, if not already available, is bound to be in circulation soon.

**Finding Solutions – ongoing efforts in the technological and legal spheres**

In the face of such stark threats, a proactive and robust approach to privacy is urgently required. Scholars and lawmakers have recognized the need for sustained debate. Computer scientists and mathematicians have attempted to devise technological means of privacy protection, including encryption, privacy preserving data mining, and anonymous cash transfer.

However, certain privacy challenges are not capable of being resolved technologically. Face-recognition software, for instance, cannot be prevented from performing through technological methods. Camera surveillance cannot be curbed technologically. And RFID monitoring cannot be forcibly defeated. In addition, certain situations require that private information be disclosed to select parties. After disclosure has occurred, the integrity of the information depends on the willingness of these parties to respect its sensitive nature. A certain measure of trust is thus always a part of most private exchanges, and trust cannot be enforced technologically. There is thus a need for legislative action to compensate for the deficiencies of technological solutions.

The government has been receptive to the demands made of it by privacy advocates. A search for the keyword “privacy” on http://thomas.loc.gov, a legislative database maintained by the Library of Congress, returns more than 50 hits for bills in the current Congress alone. Titles include the *Wireless 411 Privacy Act (S.1973.IS)*, the *Patient Privacy Act (H.R.1699.IH)*, and the *Consumer Privacy Protection Act of 2003 (H.R.1636.IH)*. Broadly speaking, Gellman identifies three sources of legal privacy protection: “constitutional protections, common-law remedies, and statutes that attempt to address privacy concerns.”

A review of privacy legislation is not possible within the scope of this paper. Yet such legislation has been prolific – starting with the *Fair Credit Reporting Act* of 1970 that Gellman highlights as “the first privacy law of the modern age” – and has helped in holding the fort against increasingly severe challenges.

**Deficiencies of the Current Legal Approach**

However, I believe that the approach adopted by current privacy legislation efforts is problematic, and is inadequate to address emerging challenges. Broadly, the problems are as follows:

1. For starters, legal code addresses privacy on a case by case basis, and rejects or accepts violation claims on the basis of subjective analysis that is difficult to replicate ex-ante. It was difficult, for instance, to determine whether wiretapping violates privacy rights and

---

6 Gellman, 195.
7 Gellman, 202.
constitutional protections, before *Olmstead v. United States* was heard by the Supreme Court. Olmstead could not have concluded either way before the hearing; neither could the federal agents have predicted with certainty which way the ruling would go. In fact, the Olmstead ruling has since been reversed, and telephonic conversations are now considered constitutionally-protected private exchanges.

Essentially, it is unclear what will be upheld as private in a court of law. Is the fact that a person visited his doctor on a certain date protected information? Or that he purchased an HIV home-diagnostic-test at a local store? The legal stance on these issues is unclear, or at least not well known. Such uncertainty creates an ambiguous climate for privacy protection and is detrimental to proactive debate.

(2) Because the notion of privacy is vaguely defined, it is difficult to articulate in legal code what is and is not private. It is even tougher to constantly update this nebulous notion of privacy in the face of evolving technology. As discussed, changes in technology can greatly modify the existing privacy landscape, and it is thus extremely difficult to write laws that will continue to be instructive in the future.

Consider an example from recent legislation. The *Privacy Act of 2003* does not protect biometric identifiers, such as retinal scans, as privileged information.8 Clearly there is widespread concern that biometric information poses privacy challenges, but the law has not been able to address this issue successfully (perhaps because these challenges are not yet concrete enough to be legally codable).

(3) Legislation and legal codes generally outline what *cannot* be done with private information. For instance, the *Privacy Act of 2003* states that "It is unlawful for a commercial entity to collect personally identifiable information and disclose such information to any nonaffiliated third party for marketing purposes [...]."9 Such narrow definitions of privacy related activities are bound to run into trouble, because it is hard to foresee potential loopholes-in/threats-to proposed laws at the time of legislation. For instance, may we extrapolate from the *Privacy Act* that unconditional disclosure to affiliated entities is acceptable? Neither is it exactly clear what distinguishes an affiliate from a non-affiliate.

Also, other possible privacy infringements that are not specifically articulated may, if at all, only be covered by vague guidelines – such as that "disclosure may not be damaging" – leading to exploitable ambivalence.

Gellman writes in further detail: “The American approach to privacy is sometimes called ‘sectoral.’ There are no general privacy laws, just specific laws covering specific records or record keepers. As a result, the legal structure for privacy in the United States is a patchwork quilt. This makes for more interesting analysis [as opposed to a uniform approach], although not necessarily for better privacy protection.”10 The vagueness and inflexibility implied by the points above limit the effectiveness of legal solutions to privacy challenges. Legal approaches are thus not able to make good for the inadequacy of technological approaches. When combined, the

---

9 Privacy Act of 2003, Title I, Section 101.
10 Gellman, 195.
deficiencies in both realms prevent the privacy debate from moving forward as swiftly as is required.

Looking for an Alternative

In the following pages I posit an integrated approach to privacy that attempts to comprehensively address current and future threats. The suggested scheme collectively deals with privacy issues by de-emphasizing the dissimilarities between them, and instead focusing on their underlying commonality. In response to previously raised questions, I believe that all privacy threats are inherently similar and are well suited to omnibus solutions.

I develop the approach around the abstract concept of information, believing information to be at the heart of all privacy issues. Information serves as the foundation of the approach, to the extent that securing privacy is equivalent to securing information. Information, viewed as a theoretical construct of the privacy debate, is capable of denoting a lot (if not all) of what we could wish to keep private.

Like privacy, information is hard to define. A possible approximation to a precise definition is that anything that is capable of being ‘communicated’ can be classified as ‘information’. Assume for a moment that this is the case. Now, if we wish to keep some things private, that is keep them from others, we can only be concerned about privacy violations if what we wish to protect is communicable. Thus, everything that we could be concerned about privacy-wise is a subset of information. Therefore, if we can devise a scheme to control certain information, we can effectively address certain privacy concerns.

Consider the three primary technology categories, described previously, that pose threats to privacy. It is hard to disagree that data can be classified as information. Our movements and physical coordinates are also capable of being perceived and known by a second person. And finally, our facial features, finger-prints, and DNA, also constitute communicable information.

Information as the Foundation of Privacy

From the point of view of information, then, any privacy debate is a discussion about (1) what information should be considered private, and (2) the means of safeguarding such information. Both parts are inherently problematic.

Steps to safeguard privacy, for instance, often need to be coercive and one-sided. The party that information is being withheld from may not assent to being denied access – this party may attempt to defeat protective measures or to forcibly obtain disclosure. It is in this sense that Westin writes that privacy is a matter of “interests and power.”

The other part is equally intractable, and has constantly tested legal scholars. Can a person decide, for instance, that his facial features are private information? Can this person expect others to respect his decision? Should he be allowed to coercively enforce safeguards? Should a court of law award him damages against someone who attempts to invade this solitude? Women in some persuasions of Islam answer yes to the above when they choose to wear burkas in public spaces. Other societies may be less certain about these and similar questions. In fact, U.S. courts have had trouble deciding whether trash-bags left on curbs embody private information.

A License Based Privacy-Protection Scheme

An alternative to mandating universal normative standards is to allow individuals to make personal choices about the privacy issues before them. That is, a person should be able to decide
which pieces of information that originate with him or belong to him (essentially, pieces of information that are communicated by him) are private, and which ones are not. He should then be able to dictate what can and cannot be done, after disclosure, with the pieces that he designates as private.

Such control is easy to achieve for threats that emerge from technologies in class (A), since this class deals with data. I posit a scheme that allows for fine-grained control over data, and that leaves the nuances of disclosure up to the individual. Specifically, I propose creating the following licenses for conditional disclosure:

**License 0**: The license assigned by default to the origin of a particular piece of data. The holder of a class 0 license may bestow, upon second parties, licenses of other classes for that data.

**License 1**: A license for particular data bestowed upon an entity, that permits that entity to view/process the data, and to distribute it to other entities under a class 1 license. (*Unbounded Distribution*)

**License 2**: A license that allows an entity to view/process the data, and to distribute it to other entities for viewing only (recipients may not further distribute the data). (*Bounded Distribution*)

**License 3**: A license that allows an entity to view/process the data, and to distribute it to other entities for one-time viewing/processing (recipients must destroy the data after the initial viewing). (*Bounded Decaying Distribution*)

**License 4**: A license that allows an entity to view/process the data. (*Persistent Disclosure*)

**License 5**: A license that allows an entity to view/process the data once (the data must be destroyed after viewing). (*Decaying Disclosure*)

**Applying Licenses to Everyday Data Disclosures**

Individuals can use these licenses as tools to tailor everyday data disclosures to their subjective privacy preferences. For instance, if you are disclosing your annual income to a credit card company for the purpose of card issuance, you may require that this data be used under license-5. That is, the card company may process the data in some privacy-preserving way, complete the application, and then delete the data from its records.

Similarly, drivers’ licenses can be disclosed at bars under license-5. Social Security numbers (SS#s) may be disclosed at banks under license-4. For the purpose of running a credit check, a person may disclose his SS# to his employer under license-2.

In addition, when there is more than one piece of data, preferences may be specified for certain (or all) subsets of data. For instance, you may choose to disclose the subset containing your name, address and SS# under license-4, but also disclose the subset containing only your name and address under license-3. On forms and documents, this can be achieved by drawing boxes around particular pieces of data, and designating a particular license to all data within a box. All data outside a box can be assigned another license. Or of course, licenses can be assigned for individual pieces by using a one digit marker.

Some order of license precedence may have to be established to deal with cases where contradictory licenses are mistakenly designated for overlapping sets of data (for e.g., name and
SS# under license-4, but SS# under license-5). But this is a minor matter and can be resolved by allowing the licensee to interpret ambiguous licenses according to his convenience.

**Augmenting the Scheme**

This licensing scheme can be further augmented to allow for the addition of subjective qualifiers. For instance, a person may release data under license-2, but require that redistribution only be made to non-commercial entities. Or he may disclose data under license-4, but require that after a certain date the licensing status be changed to license-5. Further, he may disclose data under license-2, but require that this data be redistributed to at most one other entity (to complete a SS# based credit check, for instance).

**Contentious Licensing Issues**

There remains the hairy question of who has the class 0 license for some particular data? What class 0 licenses, exactly, does an individual control? Do we control our names under a class 0 license? Should every piece of data be licensed and controlled in this way? Common sense and social standards will be crucial in determining that in some cases (so the need for social consensus cannot be eliminated). But generally, if you are expected to fill out certain data on a form, then you are also expected to have a class 0 license for that data (unless you are redistributing that data under a received license).

An additional outstanding issue is that of deciding what constitutes an entity for licensing purposes. Again common sense should come to the rescue. The answer ought to be clear in most cases. But if it is not, the receiving entity should be defined as narrowly as possible, to the extent that the intended use of the disclosed data allows. Helen Nissenbaum, Associate Professor at New York University, formulates a theory of privacy in terms of spheres of contextual integrity – essentially, theoretical spaces that compartmentalize life into distinct domains. Leakage of information between domains could amount to a violation of privacy. Nissenbaum’s paper provides us with a working theory for defining entities. In fact in many ways, the posited scheme serves to operationalize Nissenbaum’s argument, making it practically applicable.

Nevertheless, through the licensing system posited here, individuals can have the ability to insist on a fine-tuned level of privacy protection. Commercial establishments, and other recipients of data, would have the option of providing that protection, losing business to competition, or paying out incentives to obtain a higher level of data control.

**Facilitating Large Scale License Use**

In order to ensure that the licenses are legally binding, a contract template can be created for each license. These templates can then be used over-and-over to enforce the required license between two particular parties, and for particular data. In addition, any required qualifiers can also be added to the contracts on a case by case basis. Generally, contracts are highly enforceable and should fulfill the legal demands of the system.

However, contracts are also cumbersome long-winded documents. The power afforded by contract formation is overkill for everyday transactions, be it online shopping or the filling out of financial forms. Everyday scenarios require concise and comprehensive means of privacy protection. The proposed scheme in itself is simple and fulfills these goals, but if a contractual document has to be furnished at each disclosure, then users may be deterred from adopting it on a large scale. It is possible, however, that if the scheme is publicized, and if standardized contract

---

templates (issues by a prominent governmental/non-governmental agency) are common knowledge, then including a reference to the template will be adequate to achieve enforceability at the time of disclosure.

It may also be useful to think in terms of congressional legislation, in order to achieve common knowledge of the licenses. By mandating that the licenses be accepted as a means of conditional disclosure, and by confirming their legal enforceability, Congress can encourage adoption of the scheme. In addition, legislation can mandate default preferences that must be used when a license is not explicitly designated. For instance, Congress may require that all disclosure be under license-4, unless stated otherwise. Such a default setting would lower the complexity of everyday transactions by reducing required paperwork, while simultaneously ensuring that the scheme is universally and uniformly applied.

**Similarities, and Differences, between the Posited Licensing Scheme and P3P**

P3P has taken a step in the direction of large scale use by encouraging universal acceptance of a straight-forward privacy scheme. P3P, and the licenses posited here, share a common core of objectives. The P3P website describes its mission as follows: “The Platform for Privacy Preferences Project (P3P), developed by the World Wide Web Consortium, is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. [...] P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see.”

By standardizing privacy settings in a machine parseable format, P3P aims to achieve conciseness and reliability in routine transactions.

Both P3P and the licenses are open-ended privacy schemes, in that they articulate a basic language and provide room for extensions. The licenses do this by allowing for qualifiers – subjective clauses that make available the whole range of contract-forming power. P3P does this through its ‘extension’ element; to quote: “P3P provides a flexible and powerful mechanism to extend its syntax and semantics using one element: EXTENSION. This element is used to indicate portions of the policy/policy reference file/data schema which belong to an extension. The meaning of the data within the EXTENSION element is defined by the extension itself.”

P3P solves the problem of defining the term ‘entity’ (in the scope of the licenses) by requiring an explicit description: “The policy element [in very policy] MUST contain an ENTITY element that identifies the legal entity making the representation of the privacy practices contained in the policy.”

In addition, every P3P policy “includes one or more statements. Each statement includes a set of disclosures as applied to a set of data elements.” By requiring the specification of disclosure preferences under this ‘statement’ tag, P3P duplicates the control over retention and distribution of data achieved by the posited licenses. More specifically, “The STATEMENT element is a container that groups together a PURPOSE element, a RECIPIENT element, a RETENTION element, a DATA-GROUP element, and optionally a CONSEQUENCE element and one or more extensions. All of the data referenced by the DATA-GROUP is handled according to the disclosures made in the other elements contained by the statement.” Thus P3P

---

12 Platform for Privacy Preferences Project (P3P), online, <http://www.w3.org/P3P/#what>.
13 P3P, online, <http://www.w3.org/TR/P3P/#extension>.
14 P3P, online, <http://www.w3.org/TR/P3P/#POLICY>.
15 P3P, online, <http://www.w3.org/TR/P3P/#POLICY>.
16 P3P, online, <http://www.w3.org/TR/P3P/#Statements>.
and the licensing scheme are analogous, especially due to their extensibility. For instance, P3P could be extended to allow for redistribution to a limited number of entities. And the licensing scheme could be qualified to allow for redistribution to a certain class of entities.

Unlike the licenses however, all of P3P’s elements are highly articulated over the domain of web-use. That is to say, P3P’s syntax is suited to privacy concerns arising out of web browsing. For instance, the ‘purpose’ element can be set to ‘Web Site and System Administration,’ or ‘One-time Tailoring’ (among others).

In addition, unlike the licenses, P3P fails to allow individuals to make subjective privacy decisions. Web-surfers are only able to accept or reject furnished privacy policies. Such a binary decision making mode fails to capture the continuum of privacy preferences encountered in everyday life.

**Expanding the Scope of the Posited Scheme to Non-Textual Scenarios**

The challenge thus lies in creating a scheme that can accommodate most (if not all) real-world privacy considerations. The licenses posited above seek to do that for data, and for technologies belonging to threat category (A).

The next step is to extend these licenses to categories (B) and (C). One reason why category (A) has been easy to deal with, is that data is an easy-to-describe form of information. Being textual in nature, data is easy to identify when encountered. Therefore the transmission of data, whenever it occurs, is explicit and overt. The problem with technologies in categories (B) and (C) is that most of the information that they collect is non-textual – information that is a by-product of ordinary activities. Individuals are usually not conscious of being monitored by these technologies, and are therefore unable to mediate in the process. If a person is aware that he is being tracked by an RFID tag, he may at least demand removal of the tag (or he may accept the tracking) – but when tracking is surreptitious, even the basic ‘yes/no’ mode of binary decision making is not available.

Therefore the first step to extending the licensing scheme to categories (B) and (C) is to legally require prior notification of surreptitious surveillance and information gathering. Doing so would give individuals a chance to control the information that originates with them. In addition to simply prohibiting or accepting collection, with notification it will be possible to avail of the whole spectrum of privacy possibilities embodied in the posited licenses. For instance, when confronted with the fact that surveillance cameras are in operation, an individual may use any one of the proposed licenses to specify what can be done with the recordings. If the camera operators agree to the individual’s terms, then the two parties have formed a contract and are obligated to adhere to its provisions. If the individual’s terms are not acceptable to the operators, then the individual has the option of leaving the monitored space, or alternately, staying and consenting to unconditional disclosure. Essentially, prior notice creates an opportunity for consideration, and therefore for contract formation.

Some consensus will have to be reached about when notice is required. Naturally, notice cannot be demanded for all instances of information disclosure. For instance, an individual cannot expect notice when passers-by observe the license plate number on his car. But indeed, he may expect notice when a camera system is being used to log the entry and exit of all cars in a parking lot.
Moving Towards a Comprehensive Forward-Looking Approach

A sensible option is to require notification whenever technology is used to facilitate information collection that would not be possible without that technology. This would go a long way in tilting the privacy landscape in favor of individuals. Such notification would ensure that individuals can invoke the licensing scheme to make subjective choices on a case-by-case basis, whenever technology threatens their privacy.

Another, less stringent, option is to extend the subjective-objective expectation standard vis-à-vis governmental agencies, to non-governmental entities (interpreted generously, one would hope, in favor of individuals, and with a highly skeptical view of any technology that is used to enhance natural perceptual abilities). Because of constitutional and common-law provisions, the government may not use technology, without a warrant, in order to obtain information that would not be available to it otherwise. Human beings are naturally endowed with certain perceptual abilities, but when technology augments and extends these abilities it creates an opportunity for governmental oppression (Orwell). The same opportunities for exploitation exist when non-governmental agencies wield such technologies. Thus non-governmental agencies should also be prevented from surreptitiously using invasive technologies against individuals.

Constitutional grounding for such an extension may be hard to find. But there is at least some legal sanction for the goals achieved by applying the proposed licenses to all threatening technologies. In his famous law review article, Brandeis discusses privacy expectations and provides us with a set of privacy objectives relevant in all scenarios:

The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. Under our system of government, he can never be compelled to express them (except when upon the witness stand); and even if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them. The existence of this right does not depend upon the particular method of expression adopted. It is immaterial whether it be by word or by signs, in painting, by sculpture, or in music. Neither does the existence of the right depend upon the nature or value of the thought or emotions, nor upon the excellence of the means of expression. The same protection is accorded to a casual letter or an entry in a diary and to the most valuable poem or essay, to a botch or daub and to a masterpiece. In every such case the individual is entitled to decide whether that which is his shall be given to the public. No other has the right to publish his productions in any form, without his consent. This right is wholly independent of the material on which, the thought, sentiment, or emotions is expressed. It may exist independently of any corporeal being, as in words spoken, a song sung, a drama acted. Or if expressed on any material, as in a poem in writing, the author may have parted with the paper, without forfeiting any proprietary right in the composition itself. The right is lost only when the author himself communicates his production to the public — in other words, publishes it.

Technology should not be permitted to surreptitiously overturn this status quo.

---

18 Brandeis, “The Right to Privacy.”