Privacy and Civil Liberties

1. Privacy

Computer and information technology, like other new technologies, creates new possibilities; it creates possibilities for behavior and activities that were not possible before the technology. Computers made it possible (and in many cases, cheap and easy) to gather detailed information about individuals to an extent never possible before. Public concern about computers and privacy arises for precisely this reason. Of all the social and ethical concerns surrounding computer technology, the threat to personal privacy was probably the first to capture public attention. And this issue persists in drawing public concern and leading to action by policy makers.

1.1. Panopticon: an old age Privacy issue

Panopticon is the word Jeremy Bentham used in 1787 to describe his idea for the design of prisons. In the panopticon, prison cells would be arranged in a circle and the side of each cell facing the inside of the circle would be all glass. The guard tower is placed in the center of the circle, from which every cell is in full view. Everything going on in each cell can be observed. The effect is not two-way; that is, the prisoners can not see the guard in the tower. The idea of the panopticon was picked up by Michel Foucault in 1975 and brought to wider public attention. Bentham and Foucault recognized the power of surveillance to affect the behavior of individuals. In the panopticon, a prison guard need not even be there at every moment; when prisoners believe they are being watched, they adjust their behavior. When individuals believe they are being watched, they are compelled to think of themselves as the observer might think of them. This shapes how individuals see themselves and leads them to behave differently than they might if they weren't being observed.

1.2. Privacy then and now

Nowadays, the central, state, and local government agencies maintain extensive records of individual behavior including such things as any interaction with criminal justice agencies, income taxes, employment history , use of human services agencies, motor vehicle registration, and so on. As well, private organizations maintain extensive databases of information on individual purchases, airline travel, credit worthiness, health records, telephone or cellular phone usage,

The only differences between what is now possible through IT and what was envisioned then is that much of the record keeping is done through electronic records instead of by direct human observation or through cameras.

So, it seems like we are building a panopticon in which everything we do is observed and could come hack to haunt us.

2. Information Technology has changed Record Keeping

Computer technology has changed record-keeping activities in a number of undeniable and powerful ways.

1. The scale of information gathering has changed.
2. The kind of information that can be gathered has changed.
3. The scale/exchange of information has changed enormously.

In the pre-computer 'paper-and-ink' world, there were limitations on the amount of data gathered, who had access, how long records were retained, and so on. Electronic records do not have those

imitations. We can collect, store, manipulate, exchange, and retain practically infinite quantities of data.

The kind of information that it is now possible to collect and use is also infinite. Employers can keep records of every keystroke an employee makes. Employers can monitor their employees' uses of the Web, their participation in chat rooms, not to mention their e-mail. Transaction Generated Information (TGI) are also new form of information, which includes purchases made with a credit card, telephone calls, entry and exit from intelligent highways, and so on. TGI can automatically be recorded.

In addition to the scale and kind of information gathered with computer technology, there is yet another element - copy and distribution. Now information can go anywhere in the world through communication media. Hence, the extent to which information can be exchanged is now practically limitless. Once information about an individual is recorded in a machine or on a disk, it can be easily transferred to another machine or disk. It can he bought and sold, given away, traded, and even stolen. The information can spread instantaneously from one company to another or, one sector to another, and from one country to another.

3. Computers and Privacy Issues

3.1. Uses of Information

The computers and privacy issue is often framed as an issue that calls for a balancing of the needs of those who use information about individuals (typically government agencies and private institutions) against the needs or rights of those individuals. Information is created, collected and exchanged because organizations can use it to their interests and activities. Information about individuals is used to make decisions about those individuals, and often the decisions profoundly affect the lives of those individuals whom the information is about.

In general, those who want information about individuals want it because they believe that it will help them to make better decisions. For instance, banks believe that the more information they have about an individual, the better they will be able to make judgments about that individual's ability to pay back a loan or about the size of the credit line the individual can handle.

Personal privacy is generally put on the other side of the balancing scales. The issue is framed so that we have to balance all the good things that are achieved through information gathering and exchange against the desire or need for personal privacy. Some even claim that we have a right to personal privacy for if that were true, the scales would weigh heavily on the side of personal privacy. From a legal and constitutional point of view, however, we have, at most, a limited and complex right to privacy.

This framing of the issue seems to be skewed heavily in favor of information gathering and exchange. The only way to counter the powerful case made on behalf of information gathering and exchange is, it would seem, to make a more powerful case for protecting and ensuring privacy in the lives of individuals. Either we must show that there is a grave risk or danger to these information-gathering activities - a danger so great that it counterbalances the benefits of the activity. Or we must show that there is a greater benefit to be gained from constraining these activities. To put this another way, once the benefits of information gathering and exchange are on the table, the burden of proof is on privacy advocates to show either that there is something harmful about information gathering and exchange or that there is some benefit to be gained from constraining information gathering, Either way, there is a daunting hurdle to overcome.

Many of us feel uncomfortable with the amount of information that is gathered about us. We do not like not knowing who has what information about us and how it is being used. Why are we so uncomfortable? What do we fear? Part of the fear is, no doubt, related to our mistrust of large, faceless organizations, and part of it is related to mistrust of government. The challenge is to

translate thus discomfort and fear into all argument that counterbalances the benefits of information gathering.

3.2. Personal Privacy

Two big questions have dominated the philosophical literature on privacy:

1. What is it?
2. Why is it valuable?

The term privacy seems to be used to refer to wide range of social practices and domains. For example, what we do in the privacy of our own homes, domains of life in which the government should not interfere, things about ourselves that we tell only our closest friends. Privacy seems, also, to overlap other concepts such as freedom or liberty, seclusion, autonomy, secrecy, controlling information about ourselves. So, privacy is a complex and, in many respects, elusive concept.

As we review several of these, it will be helpful to keep in mind a distinction between privacy as an **instrumental good** and privacy as an **intrinsic good**. When privacy is presented being valuable because it leads to something else, then it is cast as an instrumental good. In such arguments, privacy is presented as a means to an end. Its value lies in its connection to something else. On the other hand, when privacy is presented as good in itself, it is presented as a value in and of itself. As you might predict, the latter argument is harder to make for it requires showing that privacy has value even when it leads to nothing else or even when it may lead to negative consequences.

The arguments on behalf of privacy as an instrumental good begin to cross into privacy as an intrinsic good when they suggest a connection between privacy and autonomy. If privacy were essential to autonomy, then the loss of privacy would be a threat to our most fundamental values. The connection between privacy and autonomy is often presented not exactly as a means-ends relationship. Rather the suggestion is that autonomy is inconceivable without privacy.

3.3. Information Mediates Relationships

People need to control information about themselves in order to maintain a diversity of relationships. The insight is that individuals maintain a variety of relationships (e.g., with parents, spouses employers, friends, casual acquaintances, and so on) and each of these relationships is different because of the different information that each party has. These diverse relationships are a function of differing information.

3.3.1. Individual-Individual Relationships

If everything were open to all (that is, if everyone knew the same things about you), then diversity would not be possible. You would have similar relationships with everyone. We control relationships by controlling the information that others have about us. When we lose control over information, we lose significant control over how others perceive and treat us. However, the information gathering and exchange that goes on via computer technology does not seem, on the face of it, to threaten the diversity of personal relationships each of us has. For example, despite the fact that huge quantities of data now exist about purchases, phone calls, medical condition, work history, and so on, one is able to maintain a diversity of personal relationships.

3.3.2. Individual-Organization Relationships

Private and public organizations are powerful actors in the everyday lives of most individuals in our society, and yet it would seem that individuals have very little power in those relationships. One

major factor making this possible is that these organizations can acquire, use, and exchange information about us, without our knowledge or consent.

Individuals control what relationships they have and the nature of those relationships by controlling the flow of information to others; when individual have no control over information that others have about them, there is a significant reduction in their autonomy.

3.4. Privacy as a Social Good

Priscilla M. Regan, in her book, *Legislating Privacy*, examined three privacy policy debates that took place in the United States in recent years—

- information privacy,
- communications privacy, and
- psychological privacy.

She concludes that while an individual privacy is pitted against social goods such as law enforcement or government efficiency, personal privacy loses. Regan suggests that privacy should be seen not as an individual good but rather as a social good. As an important social good, privacy would be on par with other social goods such as law enforcement or government efficiency. Instead of a social good outweighing an individual good, it would be clear that we have two social goods at stake. In reframing the issue in this way, privacy would be much likely to be treated as equally important, if not more important, than other social goods.

4. Privacy Protection

Here are a few proposals in favour of the privacy protection.

4.1. Broad Conceptual Changes and Legislative Initiatives

One is to think of privacy as a social good at the heart of liberal democratic societies and hence to be given much more weight in balancing of social goods. To make this shift is to move from seeing privacy as simply something individuals want for their personal protection, but not worth the cost in terms of inefficiency to recognizing privacy's role in democracy and, hence, recognizing that it is worth what it may cost in terms of less efficient institutions,

The United States has taken a piecemeal, ad hoc approach to information privacy with each sector being dealt with separately. Significant improvement could be had by taking a comprehensive approach and developing legislation that lays out the parameters for public anti private information gathering. Such legislation should be made with an eye to global exchange of information.

Legislations of privacy can be made in the constitution. The first one is **the freedom of speech and the press**, while the second will proscribe **unreasonable search and seizure**, and insults security in person, houses, papers, and effects. These two deal with the relationship between the government and the press, and the government and the individual.

4.2. Computer Professionals

Computer professionals can play an important role, individually and collectively. First and foremost, individual professionals must not wash their hands of privacy issues, For example, a computer professional can point out privacy matters to clients or employers when building databases containing sensitive information. Whether or not computer professionals should refuse to build systems which they judge to be insecure is a tough question, but certainly one that ought to be considered an appropriate question for a 'professional.'

Individually and collectively, computer professionals can inform the public and public policy makers about privacy/security issues, and they can take positions on privacy legislation as it pertains to electronic records. computer professionals are often in the best position because of their technical expertise, to evaluate the security of databases, and the potential uses and abuses of information.

The original ACM Code of Professional Conduct is also guided by privacy protection concepts. One if the General Moral Imperatives of the 1992 ACM Code of Ethics and Professional Conduct is that an ACM member will 'Respect the privacy of others." The Guidelines explain that: "It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals."

4.3. Technology

Related to the contribution of computer professionals is the potential of technology to protect rather than erode privacy. Privacy enhancing technologies (sometimes referred to as PETs) are now being developed. Computer scientists and engineers have been working on and have developed IT tools that allow one to navigate the Web with anonymity; to send e-mail anonymously through anonymous remailers; or to detect the privacy level of Web sites before one accesses them. More generally cryptographic techniques are being developed with various schemes that could allow one to make various transactions such as banking, purchasing, and so on, with confidentiality or to authenticate mail of various kinds.

4.4. Institutional Policies

Where no law applies or the law is unclear, private and public organizations can do a great deal to protect privacy by adopting internal policies with regard to the handling of personal information. Computer professionals working in such organizations can recommend and support such policies. For example, banks, insurance companies, registrars' offices of universities, marketing agencies, and credit agencies should have rules for employees dealing with personal information. They ought to impose sanctions against those who fail to comply. It is not uncommon now to hear of employees who casually reveal interesting information about individuals that they discover while handling their records at work.

4.5. Personal Actions

It will not he easy, and may be quite costly, for individuals to achieve a significant degree of personal privacy in our society. Gary Marx (1991) has provided a list of steps that individuals can take. His list includes the following:

(1) Don't give out any more information than is necessary;

(2) don't say things over a cellular or cord less phone that you would mind having overheard by strangers;

(3) ask your bank to sign an agreement that it will not release information about your accounts to anyone lacking legal authorization and that in the event of legal authorization, it will contact you within two days;

(4) obtain copies of your credit, health, and other records and check for accuracy and currency;

(5) if you are refused credit, a job, a loan, or an apartment ask why (there may be a file with inaccurate, incomplete, irrelevant information);

(6) remember that when you respond to telephone or door-to-door surveys, the information will go into a databank; and

(7) realize that when you purchase a product or service and file a warranty card or participate in a rebate program, your name may well be sold to a mailing-list company.

Source:

? Deborah G. Johnson, *Computer Ethics*, Third Edition