Privacy and Cybertechnology

- Privacy issues involving cybertechnology affect all of us, regardless of whether we have ever owned or even used a networked computer.

- Consider the amount of personal information about us that can be acquired from our commercial transactions in a bank or in a (physical) store.
Privacy and Cybertechnology (Continued)

- Also, consider that closed circuit television cameras (CCTVs) located in public places and in shopping malls record many of your daily movements as you casually stroll through those environments.

- Current Web-based applications such as Google Street View (a feature of Google Earth and Google Maps) enable users to zoom in on your house or place of employment and potentially record information about you.
Even if you use the Internet solely for recreational purposes, your privacy is threatened.

Personal data, including data about our Web-browsing interests, can now easily be acquired by organizations whose need for this information is not always clear.

A user’s personal data acquired via his/her online activities can be sold to third parties.
Privacy concerns now affect many aspects of our day-to-day lives – from commerce to healthcare to work.

So, we have categories such as:

- Consumer privacy,
- Medical/healthcare privacy,
- Employee/workplace privacy.
Are any privacy issues unique to cybertechnology?

Privacy concerns have been exacerbated by cybertechnology in at least four ways, i.e., by the:

- **Amount** of personal information that can now be collected;
- **Speed** at which personal information can now be transferred and exchanged;
- **Duration** of time in which personal information can now be retained;
- **Kind** of personal information (such as transactional information) that can be acquired.
What is Personal Privacy

- Privacy is a concept that is difficult to define.
- We sometimes speak of an individual’s privacy as something that can be:
  - lost, or diminished,
  - intruded upon, or invaded,
  - violated, or breached.
What is Privacy (continued)?

- Privacy is sometimes viewed in terms of something that can be *diminished* (i.e., as a repository of personal information that can be eroded gradually) or *lost* altogether.

- Privacy is sometimes also construed in terms of the metaphor of a (spatial) zone that can be *intruded upon* or *invaded*.

- Privacy is also sometimes analyzed in terms of concerns affecting the confidentiality of information, which can be *breached* or *violated*. 
Classic Theories of Privacy

- Traditional (or classic) privacy theories have tended to view privacy in connection with notions such as:
  - Non-intrusion (into one’s space),
  - Non-interference (with one’s decisions),
  - Having control over/restricting access to one’s personal information.
Non-intrusion Theories of Privacy

- Non-intrusion theories view privacy as either:
  - Being let alone,
  - Being free from government intrusion (into one’s physical space).

- This view is also sometimes referred to as *accessibility privacy* (DeCew, 1997).
The rationale for non-intrusion theories can be found in both:

- The Fourth Amendment of the U.S. Constitution (i.e., search and seizure of one’s papers, affects, and so forth);

Non-interference Theories of Privacy

- Non-interference theories view privacy in terms of freedom from interference in making decisions.

- This view of privacy is also sometimes referred to as decisional privacy.
Informational privacy is concerned with protecting personal information in computer databases.

Most people wish to have some control over their personal information.

In some cases, “privacy zones” have been set up either to restrict or limit access to one’s personal data.
### Three Views of Privacy

<table>
<thead>
<tr>
<th>Privacy Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accessibility Privacy</strong></td>
<td>Privacy is defined in terms of one's physically &quot;being let alone,&quot; or freedom from intrusion into one's physical space.</td>
</tr>
<tr>
<td><strong>Decisional Privacy</strong></td>
<td>Privacy is defined in terms of freedom from interference in one's choices and decisions.</td>
</tr>
<tr>
<td><strong>Informational Privacy</strong></td>
<td>Privacy is defined as control over the flow of one's personal information, including the transfer and exchange of that information.</td>
</tr>
</tbody>
</table>
A Comprehensive Account of Privacy

Moor (2004) has articulated a privacy theory that incorporates key elements of the three classic theories:

- Accessibility privacy (non-intrusion),
- Decisional privacy (non-interference),
- Informational privacy (controlling/restricting access to one’s personal information).
Moor’s Comprehensive Theory of Privacy

According to Moor

“an individual has privacy in a situation if in that particular situation the individual is protected from intrusion, interference, and information access by others.”
Moor’s Theory of Privacy (continued)

- A key element in Moor’s definition is his notion of a *situation*, which can apply to a range of contexts or “zones.”

- For Moor, a situation can be an “activity,” a “relationship,” or the “storage and access of information” in a computer or on the Internet.
Moor’s Privacy Theory (continued)

Moor also distinguishes between “naturally private” and “normatively private” situations required for having:
- Natural privacy (in a descriptive sense);
- A right to privacy (in a normative sense).
Applying Moor’s Natural vs. Normative Privacy Distinction

- Using Moor’s natural/normative privacy distinction, we can further differentiate between a:
  - *Loss of privacy*,
  - *Violation of privacy*. 
Descriptively Private vs. Normatively Private Situations

- Review Scenario 5-1 (in the textbook), where Tom walks into the computer lab (when no one else is around) and sees Mary in the lab.
  - In this natural/descriptively private situation, Mary’s privacy is lost but not violated.
- Review Scenario 5-2, where Tom peeps through the keyhole of Mary’s apartment door and sees Mary typing at her computer.
  - In this normatively private situation, Mary’s privacy is not only lost but is also violated.
Nissenbaum’s Theory of Privacy as “Contextual Integrity”

Nissenbaum’s privacy framework requires that the processes used in gathering and disseminating information are

- “Appropriate to a particular context”
- Comply with norms that govern the flow of personal information in a given context.
Nissenbaum’s Theory (Continued)

- Nissenbaum (2004a) refers to these two types of informational norms as:
  - Norms of appropriateness,
  - Norms of distribution.
Nissenbaum’s Theory (Continued)

- *Norms of appropriateness* determine whether a given type of personal information is either appropriate or inappropriate to divulge within a particular *context*.
- *Norms of distribution* restrict or limit the flow of information within and across *contexts*.
- When either norm is “breached,” a violation of privacy occurs.
- Conversely, the *contextual integrity* of the flow of personal information is maintained when both kinds of norms are “respected”
Nissenbaum’s Theory (Continued)

- Like Moor’s privacy model, Nissenbaum’s theory demonstrates why we must always focus on the *context in which information flows, not the nature of the information itself*, in determining whether normative protection is needed.

- Review Scenario 5-3 (in the textbook) on Professor Robert’s seminar, which illustrates the notion of “contextual integrity.”
Can Privacy Be Preserved in the Digital Era?

- In 1999, Scott McNealy, CEO of Sun Microsystems, uttered his now famous remark to a group of reporters: *You have zero privacy anyway. Get over it.*
- Froomkin (2000), Garfinkel (2000), and others have expressed concerns about the “death of privacy.”
- But some believe that not all has yet been lost in the battle over privacy.
  - For example, some privacy advocates staunchly believe that we should be vigilant about retaining and safeguarding what little privacy we may still have.
Is Protecting Personal Privacy Still Considered an Important Goal?

- Can the current privacy debate be better understood in terms of differences that reflect *generational* attitudes?
- For many “Millennials,” who are now college-aged, privacy does not always seem to be of paramount importance.
  - Consider, for example, that many Millennials seem eager to share their personal information widely on social networking services such as Facebook.
- But for many older Americans, including Baby Boomers, privacy is still highly valued.
- So the relative importance of privacy may vary considerably among the generations, at least in the U.S.
What Kind of Value is Privacy?

Three distinct questions can be distinguished with respect to privacy as a value:

- Is privacy an *intrinsic* value, or is it an *instrumental* value?
- Is privacy *universally* valued, or is it valued mainly in Western industrialized societies (where greater importance is placed on the individual than on the broader community?)
- Is privacy an important *social* value (as well as an individual value)?
Is Privacy an Intrinsic Value or an Instrumental Value?

- Is privacy something that is valued for its own sake?
  - In other words, is it an *intrinsic value*?
- Or, is privacy valued as a means to some further end?
  - Is it merely an *instrumental value*?
Is Privacy an Intrinsic or an Instrumental Value (Continued)?

- Privacy does not seem to be valued for its own sake, and thus does not appear to have intrinsic worth.

- But privacy also seems to be more than merely an instrumental value because it is *necessary* (rather than merely *contingent*) for achieving important human ends (Fried, 1990).
Is Privacy an Intrinsic or an Instrumental Value (Continued)?

- Fried notes that privacy is necessary for important human ends such as *trust* and *friendship*.

- Moor views privacy as an expression of a “core value” – viz., *security*, which is essential for human flourishing.
Privacy as a Universal Value

- Privacy has at least some importance in all societies, but it is not valued the same in all cultures.
  - For example, privacy tends to be less valued in many non-Western nations, as well as in many rural societies in Western nations.
  - Privacy also tends to be less valued in some democratic societies where national security and safety are considered more important than individual privacy.
Privacy as an Important Social Value

- Priscilla Regan (1995) notes that we tend to underestimate the importance of privacy as an important *social value* (as well as an individual value).
- Regan believes that if we frame the privacy debate in terms of privacy as a social value (essential for democracy), as opposed to an individual good, the importance of privacy is better understood.
We examine three techniques that threaten privacy:

- **Data-gathering** techniques used to collect and record personal information, often without the knowledge and consent of users.

- **Data-exchanging** techniques used to transfer and exchange personal data across and between computer databases, typically without the knowledge and consent of users.

- **Data-mining** techniques used to search for patterns implicit in large databases in order to generate consumer profiles based on behavioral patterns discovered in certain groups.
Cybertechnology Techniques Used to Gather Personal Data

- Personal data has been gathered at least since Roman times (census data).
- Roger Clarke uses the term *dataveillance* to capture two techniques made possible by cybertechnology:
  - a) Surveillance (data-monitoring),
  - b) Data-recording.