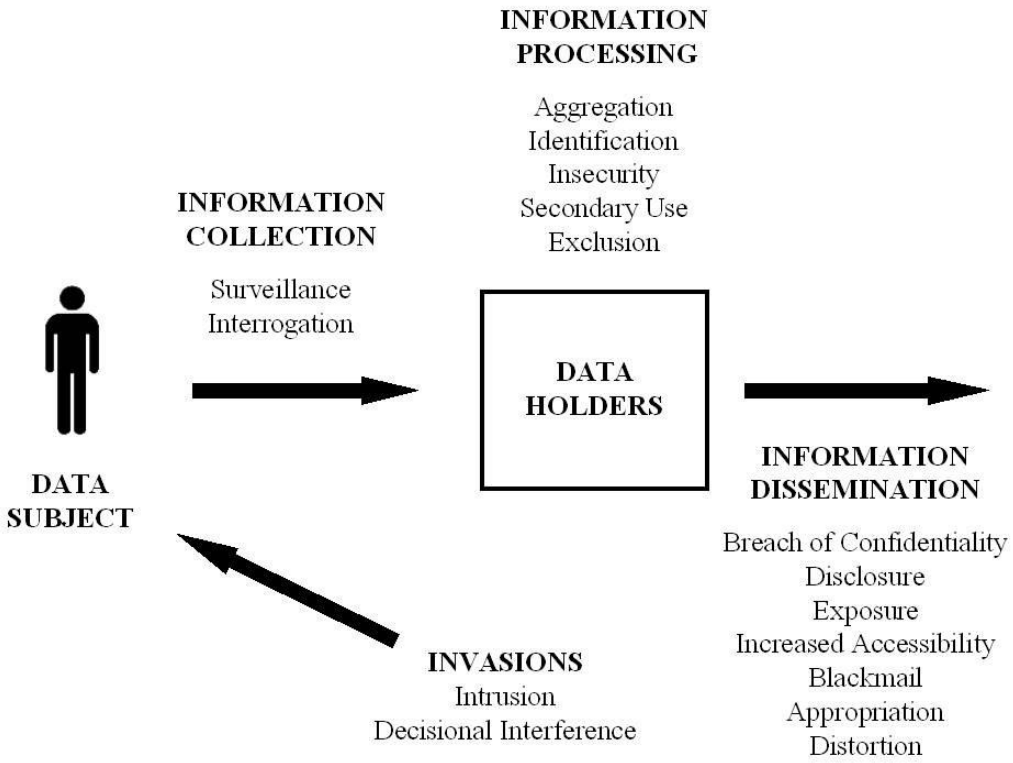
PROFESSOR SOLOVE'S TAXONOMY OF PRIVACY

Adapted from Daniel J. Solove, UNDERSTANDING PRIVACY (Harvard University Press 2008).

Privacy is a product of norms, activities, and legal protections. Privacy is about respecting the desires of individuals where compatible with the aims of the larger community. Privacy is not just about what people *expect* but about what they *desire.* Privacy is not merely an individual right – it is an important component of any flourishing community.

Privacy is not one thing, but a cluster of many distinct yet related things. Below is Professor Solove's taxonomy of the different kinds of related activities that fall under the rubric of privacy:



None of these activities are inherently bad. Nor is privacy inherently good. The interests that sometimes conflict with privacy – free speech, security, transparency, and efficient consumer transactions – are all quite valuable. We must balance the value of privacy and conflicting interests to determine which should prevail in any particular situation.

In many cases, protecting privacy does not involve a zero-sum tradeoff. We can protect privacy without sacrificing a conflicting interest if we have procedures and limitations that address the problems. For example, the Fourth Amendment protects privacy not by forbidding the government from searching but by requiring procedures of oversight and limitation.

Information Collection

The means and process of gathering data can create privacy problems.

Surveillance is the watching, listening to, or recording of an individual's activities. It can chill expression and political activity, give too much power to the watchers, and make people feel creepy and inhibited.

Interrogation consists of various forms of questioning or probing for information. It can be too prying and coercive in some circumstances.

Information Processing

Those who hold personal data process it -- they store it, combine it, manipulate it, search it, use it, and do many other things with it. The manner in which they process personal data can create a host of privacy problems.

Aggregation involves the combination of various pieces of data about a person. Aggregation can create a privacy problem because combining data can reveal facts about a person that are not readily known and that a person did not expect to be known when providing the data.

Identification is linking information to particular individuals. Identification can inhibit one's ability to be anonymous or pseudonymous.

Insecurity involves carelessness in protecting stored information from being leaked or improperly accessed. This makes people more vulnerable to fraud and identity theft.

Secondary use is the use of information collected for one purpose for a different purpose without a person's consent. Secondary creates a harm, as it involves using information in ways a person does not consent to and might not find desirable.

Exclusion concerns the failure to allow people to know about the data that others have about them and participate in its handling and use. Exclusion reduces accountability among the entities that maintain records about individuals.

Information Dissemination

Privacy problems can be created when personal data is transferred or disclosed – and even when there is a threat it will be exposed. The nature of the dissemination can create many different problems:

Breach of confidentiality is breaking the promise to keep a person's information confidential.

Disclosure involves the revelation of truthful information about a person.

Exposure involves revealing another's nudity, grief, or bodily functions.

Increased accessibility is amplifying the accessibility of information. Much of our information is protected by practical obscurity – it's hard to find it. By taking the needles out of the haystack, we greatly increase the exposure of people's personal information.

Blackmail is the threat to disclose personal information. With blackmail, the harm is not in the actual disclosure of the information, but in the control exercised by the one who makes the threat.

Appropriation involves the dissemination of certain information about a person to serve the aims and interests of another.

Distortion consists of the dissemination of false or misleading information about individuals. Many privacy statutes have provisions for the accuracy of personal information in record systems.

Invasion

Certain activities create impingements directly to the individual, interfering with the individual's private life.

Intrusion concerns invasive acts that disturb one's tranquility or solitude.

Decisional interference involves the government's incursion into people's decisions regarding their private affairs.