Interactions: a primitive for privacy threat modeling

R. Jason Cronk, *Institute of Operational Privacy Design*

Abstract

Most discussions around privacy risks and threats begin and end with data processing, but privacy concerns predate the use of data, in the modern form, by millennia. Fundamentally, privacy exists at the boundary between the individual and others in society. It is where others interact with the individual or their proxies that privacy violations occur.

1. Interactions

The term "privacy" suffers a definitional problem, where attempts to simply conjure up a unifying definition often fall flat. Privacy violations often take on an "I know it when I see it, but can't define it" quality. In truth, privacy is an umbrella term for different interactions between an individual and others in a society, where the individual desires some measure of autonomy in defining those interactions.

Daniel Solove, in his seminal work categorizing privacy harms [1], does an excellent job of cataloging all of the different situations that could be labeled as a "privacy violation." Solove breaks down the harms into 15 distinct harms[1] and four distinct areas: Information Processing, Information Dissemination, Collection, and Invasion A common thread in all of the harms identified by Solove is the necessary involvement of an interaction between a threat actor (who threatens the at-risk individual with a harm) and the at-risk individual (or a proxy for that individual). Most readers fail to realize this common thread because they fail to see that information about an individual can be a proxy for that individual – a representation of that individual – and that the individual has a rightful desire to control interaction with that information just as they rightfully desire to control society's interaction with them directly.

1.1. Individual

The individual is the person whose privacy is threatened by a threat actor.

1.2. Threat Actor

The threat actor is the person, entity, or force whose act threatens an individual with a privacy harm. While typically a natural or legal person, the threat actor need not be either. Wind, which can blow a towel off of a person changing clothes at the beach, is the threat actor that threatens to expose the individual changing.

2. Proxies

Proxies are stand-ins for the individual; they represent the individual to the threat actor. When an intruder snoops around a home or apartment, they are invading the privacy of the homeowner or tenant, not the privacy of the home or apartment. The interaction isn't direct, but the invasion is still perpetrated against the individual; the home or apartment is a proxy. Similarly, if a threat actor calls a family member and begins questioning them about an individual, the target of the interrogation isn't the family member, it is the individual; the privacy invasion isn't against the family member, it is against the individual. While the family member might be annoyed or inconvenienced, they are not the target of the threat actor's interest, whereas the individual is, even though they weren't party to the actual interaction.

2.1. Property

The first type of proxy to consider is an individual's property. Under the Solove taxonomy of privacy harms, we can describe the application of non-information privacy harms to property.

Surveillance – In lieu of monitoring an individual, one could monitor an individual's property – say, one's house. Many people would view surveillance of one's property as a privacy violation, regardless of whether the individual is home.

Interrogation – In lieu of asking an individual a question, one could interrogate an individual's property. This may be hard to envision, because the threat actor isn't verbally asking questions. But interrogation means, in the Solove harm context, to probe for information. One could envision a threat actor probing a person's computer, trying to find information on them. This isn't an information privacy harm, as the data is irrelevant. The invasive act is the probing or interrogation of the individual's property.

Intrusion – An intrusion is an incursion into the personal space of another. The individual need not be there for the act of incursion to be a violation of one's privacy. Most

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022. August 7 -- 9, 2022, Boston, MA, USA.

[1] Solove identifies 16 distinct harms, but in this author's view, Blackmail, is miscategorized, as it is actually a subset of decisional interference.

would agree that a threat actor entering your home, without permission, when you're not home, still invades your personal space.

Decisional Interference – Decisional interference is about altering someone's decisions and denying them full autonomy in their decision-making. A threat actor could do this by acting against an individual's property. Let's consider someone who doesn't want their neighbor parking in front of their house. They could slash the car's tires every time their neighbor parks their car there. This has the effect of interfering with the neighbor's decision, but rather than interacting directly with the neighbor, the threat actor is interacting with the neighbor's property, specifically their car, to effectuate that interference.

2.2. Friends and Family

The second type of proxy to consider is an individual's friends, family, or other close relationships. Under the Solove taxonomy of privacy harms, we can also describe the application of non-information privacy harms to friends and family, as a proxy for the target individual.

Surveillance – In lieu of monitoring an individual, one could monitor an individual's family, in an attempt to learn more about the individual.

Interrogation – In lieu of asking an individual a question, one could interrogate an individual's friends. If I ask your friend where you are, I'm not probing for information about them; I'm probing for information about you. Your friend is just a proxy, an easier object of my interrogation, but not the ultimate target of my question.

Intrusion – An intrusion is an incursion into the personal space of another. This one is a bit harder, conceptually, but one could imagine a person who keeps a close circle of friends. A new person (the threat actor) then infiltrates that close circle of friends, trying to become close to them. In social media, this might occur when someone "friends" (links/connects with) all of another person's friends to gain their confidence as an "insider."

Decisional Interference – Decisional interference is about altering someone's decisions and denying them full autonomy in their decision-making. A threat actor could attempt to manipulate an individual by influencing the individual's family – calling them, harassing them – in an attempt to get the individual to make a certain decision. While the family is the object of the harassment, the individual is the target. The threat actor is trying to alter the individual's decision, denying them autonomy.

2.3. Data

Data as a proxy is, naturally, the provenance of information privacy harms, such as aggregation, exclusion, disclosure, and more, categorized by Solove under Processing and Dissemination harms. Conceptually, many people struggle with data as a proxy for an individual and tend to view data in a separate mental model. But data represents the person in a metaphysical sense. It's much easier, in many circumstances, to interact with or manipulate data than the actual person. If I want to show someone on the other side of the world what you look like, it's easier for me to send a photo of you than to fly you to the other side of the world. Data also allows for multiple threat actors to simultaneously interact with "you" more easily than they could with the physical you. If I want to find out about your habits and preferences, I can interrogate data I have about you, rather than ask you. Do you like Thai food? Your frequent geolocation data indicates that you do go to Thai restaurants frequently. Another actor could infer your propensity for risk, given the speed you travel between locations. Data is a proxy for you.

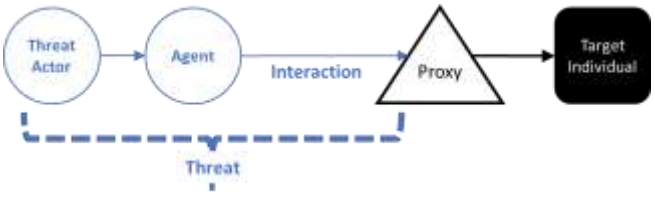
3. Agents

An additional complexity in the mix are agents. Similar to how proxies act as stand-ins for individuals, agents act at the behest of threat actors. One can analogize to a mob boss who hires a thug to go break an individual's leg. The thug is the boss's agent. Not all threat actors act directly. While generally acting at the direction of another threat actor, some agents are threat actors in their own right. For instance, employees may act on behalf of their employers and threaten individual's privacy that way, or they could go "off-script" and become threat actors, themselves.

Agents need not be natural or legal persons. Agents could include a drone (monitoring someone's movements), software, and such. Further, agents need not interact with the target; they could interact with a proxy. For instance, my drone could fly around surveilling your house when you are not even home.

4. Privacy Threats

Now that we understand the chain by which threat actors threaten individuals, we can construct a privacy threat as an interaction by a threat actor (or their agent) against an individual (or their proxy). Of course, not all interactions are threatening. Therefore, a privacy threat is an interaction that exceeds social norms of behavior, rising to the level of a known privacy harm.



Footnotes

1. Solove, Daniel J., A Taxonomy of Privacy. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006, GWU Law School Public Law Research Paper No. 129, Available at SSRN: https://ssrn.com/abstract=667622