Law Firms Must Consider Privacy Harms in the Internet of Things

Rebecca Herold and Mari Frank, Esq
eTBL Submission

The expanding use of smart gadgets in the Internet of Things (IoT) is creating many more privacy risks than ever before encountered. Many businesses and lawyers are also (finally!) starting to address privacy recognizing it is necessary to identify privacy risks are increasing and learn to do privacy risks assessments. The privacy risks to law firms and business that can occur include such things as:

- Breaches of customer and employee sensitive information resulting in expensive civil suits, costly judgements and loss of reputation
- Loss of intellectual property, including confidential case information
- Non-compliance fines by governmental agencies and possible State Bar investigations for not appropriately addressing privacy issues
- Loss of customer trust, resulting in lost business

However, law firms and other organizations must now also move into new territory and consider privacy harms. Privacy harms are those bad things that could impact individuals associated with personal information that is used for a and unconsented to purpose without the consent of the person from whom it was collected. The individuals harmed could be members of the law firm, staff, clients, opposing clients and firms, vendors and others. The privacy harm is the unanticipated or coerced use of information concerning a person against that person. These are negative, external actions by unauthorized persons with reference to personal information. Examples include identity theft, the leaking of confidential information that reveals sensitive or embarrassing facts, the theft of intellectual property. Here are just a few examples of privacy

harms, as identified by the current National Institute of Standards and Technology (NIST) Privacy Engineering initiative:

- Loss of Trust
- Loss of Self Determination
    - Loss of Autonomy
    - Exclusion
    - Loss of Liberty
    - Physical Harm
    - Emotional harm
- Discrimination
    - Stigmatization
    - Power Imbalance
- Economic Loss

Addressing privacy requires privacy harms consideration in addition to identifying security and privacy risks. This is a huge change for organizations, but most of those doing information security risk assessments aren't used to the new need to look outward from the business to consider privacy harms to associated individuals (customers, patients, etc.). When they do not do this, privacy cannot be effectively considered and mitigated. It is important for organizations to incorporate consideration of privacy risk into their PIAs and other risk management activities.

Case Study

Let's take the following scenario and run through some of the types of privacy harms that could occur to the individuals involved.

Your organization is a toy manufacturer. You are creating a new type of doll that will be leaps and bounds more evolved than the old types of dolls that talk when pulling a string. This new doll will be smart; built to interact with the children playing with them, and connected within the Internet of Things. A smart toy that will provide a way for the toy to learn from the child playing with the doll and make the doll respond to the child in ways never before possible…making the child playing with it consider the doll to be his or her best friend! These toys are going to fly off the shelves from being so popular, and will revolutionize the doll industry!!! And not only that, your organization will collect a lot of great data to determine children's likes, dislikes, trends, and another way to market our other toys through the suggestions of each child's new trusted friend. Children will be delighted, we'll increase sales; a win-win for everyone!

Here are the high-level specs for the doll:

- The doll will record everything seen and heard around it.
- The recording will be transmitted via Wi-Fi connection and stored in the organization's cloud with all the other recordings of all the other dolls that have been sold.
- Big data analysis will help each doll learn about the child that plays with it.
- The doll will be able to talk with the child using phrases and words customized to how the child talks.
- The doll will be able to ask the child questions to learn the child's likes and dislikes, where the child lives, the child's activities, and other types of information collected.
- The longer the child has the doll, the more customized the conversations can be with each child using more and more information.
- The doll will be able to suggest activities, food, movies, toys, and an unlimited number of other things to the child.

- The child's legal guardians can be given access to the own child's recordings if they want to know what the child is talking to the doll about.
- The doll can recognize the child's voice, so it will only talk with the child, and not divulge any secrets, or skew it's leaning about the child, if a different child talks to it.

Brilliant! So, what could go wrong? Well, many things. For now let's consider just a few of the potential privacy harms.

1. Loss of Trust: If the information for each child is given or sold to others (e.g., marketing companies, schools, insurance companies, mental health organizations, law enforcement, etc.) without first getting consent, consumer trust will be lost.
2. Loss of Self Determination
    a. Loss of Autonomy: The algorithm could be created in such a way that the doll may suggest activities for the child that the child would not have done otherwise, or could put the child in harm's way. This could open the company to significant liabilities.
    b. Physical Harm: If someone hacked into the system controlling what the doll says, the hacker could make the doll tell the child to do something harmful. Can you imagine of a hacker made the doll say something like, "Suzy, make your parents proud! Show them how you can shoot their gun! Get their gun and go to them, point it at them, and show them how you are such a big girl that you can pull the trigger!" Again, significant liabilities could then be faced by the company.

It could be the stuff of nightmares. The organization needs to establish policies and procedures, and build controls into their devices and products to mitigate the possibility of these privacy harms. And I didn't even touch upon privacy risks and information security risks.

Whenever an organization considers any type of new product that will interacts with users and collects information from them, privacy harms must be considered, information security and privacy policies and procedures established, and then controls implemented to mitigate them.

Mari Frank, Esq has been a lawyer since 1985. Learn more at www.MariFrank.com; www.conflicthealing.com; www.privacypiracy.org