Top 10 Ways that Big Data Increases Privacy Risks

by Julia Smith

A client asked me, "How does Big Data have an impact on customer privacy?" Answering the question helped me develop my Top 10 Big Data Privacy Risks list.

1. **The risk of re-identifying data that have been de-identified**. While the initial source data may have been scrubbed of personally identifying details, when aggregated with other sources, it enables individuals to be identified. According to a Financial Times article[1], combining just three data elements—birthday, gender, and postal code—is all that someone needs to uniquely identify at least 87% of U.S. citizens in a publicly available database. Due to the greater sophistication of new analytics tools, the risk of re-identification becomes much more likely with Big Data.

2. **The risk of deducing private information from publicly available information**. By assessing buying patterns, monitoring participation on social media sites, etc., it is possible to deduce personal lifecycle elements that an individual would rather keep private, e.g., the likelihood of pending divorce, sexual orientation. With the upsurge in data being collected and shared, this risk becomes much more likely with Big Data.

3. **The risk of data breach.** Even if an organization is using an individual's data carefully, it can fall into the wrong hands and then be used for illegal or unethical purposes. While this has always been a risk, the increased volume of data, the number of hand-off points involved in manipulating the data, the increased use of third party data brokers and cloud technologies, make Big Data analytic systems more vulnerable and tempting to hack.

4. **The risk of insider threats.** There is always the risk that people within an organization take or misuse data for personal reasons. The richness of the analytics now being drawn from Big Data sets may make this more tempting (and easier) when putting visualization and reporting tools in the hands of more people outside of a core of IT specialists.

5. **The risk of personal data being sold and shared.** While individuals may willingly grant permission for a company to use their data for a specific purpose, they may not have anticipated how that company may be sharing the data with other parties. This risk is now higher as the

rewards for monetizing valuable data are growing.

6. **The risk of personal data and analytical insights being used for unintended purposes.** While organizations are collecting and storing more and more data about buying patterns, these data can now be used for things such as legal battles, e.g., alcohol buying patterns in child custody cases, insurance claim denials based on social media postings, and so on. This risk is much greater in the Big Data world due to the volumes being collected and more sophisticated data mining tools.

7. **The risk of current personal data being used far into the future.** While people may be comfortable sharing certain information today, they may change their minds in the future. For example, a politician running for office who would rather not have her teenage son or daughter's Facebook partying pictures surface during the election. This has always been an issue but the inexpensiveness of data storage makes it more likely that companies and governments will hold on to information much longer.

8. **The risk of location tracking.** With the huge expansion of GPS trackers in phones, cars, etc., people may not be aware that their movements can, and in some cases are, being monitored. Location-based data can be used by more and more organizations, including governments. This is something which many believe is a violation of personal liberty. Government monitoring has always been present in some form, but new data sources and enhanced tools make the scope of the risk much bigger, e.g., Edward Snowden's National Security Agency (NSA) disclosures.

9. **The risk of losing customer trust unintentionally.** The tactics that companies use to help streamline marketing efforts or improve the customer experience may backfire if customers believe their data were being used in ways they (the customers) didn't think of. The potential to do more things that anger customers is much larger with the proliferation of data points and tracking tools.

10. **The risk of breaking laws or compliance issues unintentionally.** Because the business analytics market is changing so fast, the laws are still evolving and they differ from region to region. The complexity of Big Data sources, tools, and methodologies means that there is a greater risk of unintentionally being on the wrong side of the law.

Notes

I look forward to receiving comments and suggestions. For other articles, see my LinkedIn posts at Articles by Julia Smith.

1. Frank Buytendijk and Jay Heiser, "Confronting the Privacy and Ethical Risks of Big Data," *Financial Times (*September 24, 2013).

Julia Smith is an Alpha Insights Associate with over 15 years of strategy and change management consulting, executive coaching, and facilitation experience. She is strategic, creative thinker who helps shape and deliver complex technology, operations and business transformations, supplier partnerships, and process improvement initiatives. She holds an M.B.A. from Schulich School of Business, York University and a B.A. from University of Waterloo.