

Ethical Breaches – Tomorrow's Security Breach?

Douglas Hart Ph.D., Professor, College of Computer & Information Sciences, Regis University, Denver, Colorado

In 2004 the ACLU produced a videoⁱ of what ordering pizza for delivery might be like in 2015. This video has become one of the most downloaded pieces of content on the ACLU's website. Although obviously laden with satire, the video portrays a future that most find uncomfortable with the person taking the pizza order aware of the location, health, and financial information of the caller. It portrays a future where personal data is shared, used, and abused, in ways that were unimagined.

In 2014 a Whitehouse reportⁱⁱ to the president on big data and privacy outlined a wide variety of concerns about big data and privacy. For instance, the use of differential pricing for essentially the same goods, like airline tickets and college costs. Using big data information this practice could become prevalent in other market areas and at the same time become less transparent to the consumer. Another example is the use of nontraditional data sources, such as social media, in providing credit. And yet another example is tracking repeat customers in brick-and-mortar stores through their cell phones, like a browser cookie for online stores, without the consumer's awareness much less consent.

Though these examples seem a bit malevolent towards the consumer, there are also benevolent examples that nonetheless hint of privacy concerns. For example, a machine-learning algorithm to detect early signs of gambling addiction, a predictive modeling system to identify college students at risk of dropping out, or a system to analyze social media among veterans to detect those with suicidal thoughts. In these situations, interventions are warranted. But the question remains, what privacy have we relinquished unbeknownst to us?

The ethical use of data, respecting personal privacy concerns, is a central concern for today's data scientist. At most academic institutions research activities involving human subjects are governed by an ethics review that takes place before the experiments proceed. Today's data scientists and statisticians more than ever need to understand the ethical use of data and understand the potential consequences of ethical breaches for the organizations they represent. One needs only to remember the Facebook social experiment on nearly 700,000 of its users in January 2012ⁱⁱⁱ. For one week Facebook attempted to emotionally manipulate these users by showing disproportionately positive or negative status updates. Although Facebook did not suffer much in the public eye, it is not a stretch of the imagination to envision scenarios where big data experiments are revealed with organizations facing the stigma associated with today's security breaches.

Today's data science academic programs must include ethics and privacy in the curriculum. The good news is that today's students are well poised to appreciate the need for this education.

There is a social conscious within the data science community. Many of today's data scientists are using their talents for social justice concerns – to make the world a better place for all people. Witness DataLook^{iv} that showcases data-driven projects for social good, DataKind^v that seeks to find insights from data to solve seemingly complex and intractable problem that we face, and the University of Chicago Data Science for Social Good^{vi} summer fellowship program. Today's data scientists have the ability to change to world, addressing long standing problems in our communities and our society. But with great ability comes great responsibility!

ⁱ <https://www.aclu.org/ordering-pizza>

ⁱⁱ https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

ⁱⁱⁱ <http://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/>

^{iv} <http://datalook.io>

^v <http://www.datakind.org>

^{vi} <http://dssg.io>