Does It Matter if the Government is Involved? Ethical Privacy Considerations of Government Use of Social Media Data

Rebecca Balebako
Independent
Pittsburgh, PA
rebeccabalebako@gmail.com

ABSTRACT

Government agencies may wish to work with social network data. They are faced with understanding whether the ethical privacy concerns of using such data are any different for governments than for corporations. We present the common arguments that conclude that United States government use of social network data presents no additional privacy risks to American citizens. We present findings from privacy research and risk perception that indicate why concerns about government's use of data can be different from perceptions of corporate use of the same data. We argue these perceptions matter, and therefore government agencies have an extra responsibility to respect privacy concerns in the use of social network data. Given this additional responsibility, government agencies use of social network data must be carefully weighed against the social benefits such data use could bring.

Author Keywords
Privacy, risk perception, research

ACM Classification Keywords
K.4.1. Privacy, Regulation, Ethics.

INTRODUCTION

United States government agencies are often tasked with providing services to or protecting the public. Some of these services can be made more efficient with information on social connections and networks. Social network data, including information culled from social media sites such as Facebook and Twitter, or from cell phone networks can provide information useful for public policy decisions or agency decisions. For example, the public health agencies may wish to prevent the spread of deadly diseases, and understanding disease vectors could be improved by data on travel patterns and locations of people [1]. The Department of Homeland Security (DHS) has multiple concerns about border security, and may find that lists of dangerous individuals or research on characteristics of potential terrorists could help them prevent violence in the United States. As such, the DHS has begun requesting social media information from visa applicants [2]. Other agencies may wish to explore social networks to understand the spread of violent terrorism [3]. The information culled from social network data may include the content of messages, or it may be based on meta-data, such as what connections were made, when and where.

However, the use of such social network data for government work can introduce privacy concerns. The data subjects may not know or expect their contributions to be taken out of context, nor may they understand how the structure of networks that can be inferred from following, liking, or contacting others. The exact privacy concerns can depend on what data is used, how it is used, and by whom it used, among other contextual variables. In this paper, we specifically explore *who* is using the data. We explore why the ethical-privacy issues of using social network information may depend on whether government, corporations, or academia are accessing and using the information. We argue that government use of social network data should first engage a structured cost-benefit analysis that takes into consideration the risk perceptions of government use of data.

ARGUMENTS FOR GOVERNMENT USE OF SOCIAL NETWORK DATA

We argue that government use of social data confers additional ethical responsibilities on the government agencies, but not everyone agrees. In classrooms, private conversations, and workshops the author has heard statements to the effect that government use of data is no worse, or safer than corporate use of similar data. The author presents these arguments to shed light on the subject, to recognize that these perspectives exist, and to allow greater exploration of these points of view.

The first argument is that social network data is willingly posted in a public space (such as Twitter) and is therefore not private. The second argument that the privacy risks from the government use of social network data are fewer than the corporate use of such data, because U.S. government agencies have sufficient checks and balances. For example, the Privacy Act of 1974 places restrictions and requirements on government databases of personal information. These laws and others are said to ensure that objective harm to U.S. citizens from the use of their data are very small. These arguments often take the form of statements such as, “If people share so much data with corporations, they won’t care about the government using it,” and “The U.S government is so restricted in using personal data that we have little to fear.”

We suspect that many, if not all, U.S. government agencies who use social network data are indeed concerned about citizens' privacy. By dissecting the above arguments, we hope to support ethical use of social network data by U.S. government agencies. Data-driven decisions by government agencies include the possibility of improving public services or even saving lives; these benefits may outweigh the privacy risks. By outlining why the above arguments are too facile, we hope to provide a nuanced understanding of privacy concerns that enable a clearer view of the risks and benefits.

PUBLIC DATA CAN POSE RISKS

One argument is that social media data is shared with third parties, and is therefore not private. For example, some would argue that Twitter data is public because the company's privacy policy states that data will be public. In this conception, there is a strict dichotomy between public and private.

Privacy researchers argue that dichotomizing public and private ignores expectations about information use, context, and obscurity [4]. Social media users may have shared profile information with expectations that the information exists for a specific use (such as maintaining contact with old friends), in a specific context (others are also sharing and looking for similar things), and certain levels of obscurity (the profiles are available only to those who create accounts).

Furthermore, information about a person may not always be posted by that individual. In social media, one's friends and acquaintances can post information, without the user knowing or having much choice over the sharing of such information. While revenge porn is an extreme example of such sharing, other examples abound. Even friends' preferences allow inferences about private behaviors to be made about an individual [5]. This indicates that people may not have control over information about themselves, and may not be deliberately sharing publicly.

RISK PERCEPTION AND GOVERNMENT SURVEILLANCE

We now examine the idea that privacy harms from United States government use of data are less than the harms from corporate use, due to the checks, balances, and regulation that prevent U.S. government agencies from harming American citizens unjustly based on social network data. Indeed, the U.S. constitution and other laws offer protections against government intrusions into private spaces. These protections don't necessarily apply to corporations, and place restrictions on government agencies.

Nonetheless, American citizens may still *perceive* that the government could encroach upon civil liberties based on social network data. Even when objective harms are unlikely, subjective privacy harms – "the perception of unwanted observation" – may persist [6]. Subjective harms may include feelings of discomfort or levels of distrust.

People's perceptions of a risk are relevant to their behavior. To explain why perceptions of harms from the government use of social media data may differ than perception of harms from corporations' use of social media data, we highlight some relevant findings from the field of risk perception and communication.

First, it is important to note that risk perception is not always rational. People may fear technologies and perceive them as higher risk, even if that technology has a very low probability of killing them [7]. The dread or fear of a technology can still be disproportional to the actual probability of harm.

Several characteristics of a risk, outside the probability of harm, can influence a person's perceptions of risks. These characteristics include: whether the risk is undertaken voluntarily, the knowledge of the risk, the severity of consequence of the risk, and control (can the person by personal skill or diligence avoid the risks) [7].

In each of these elements, a person may feel there is a difference between sharing data with their government or sharing with a business such as a social network, or with their friends. We highlight control and severity of consequence. Alice may perceive a level of control over her data when she chooses to share it on a social network. She may perceive, rightly or wrongly, that she has a good understanding of the privacy settings and controls offered by the network, and that she controls what information she makes available. Alice may not feel this same control when her social media information is pulled by a government authority, as the government privacy settings and controls may be opaque or bureaucratic. Furthermore, while she can decide to de-active her social network account, or switch apps or technologies, it is much more difficult to switch governments. Therefore, she may not feel like she is voluntarily sharing information with the government.

Another characteristic of risk that differs between government and corporate use of data is the perceived severity of the consequence. The government has powers to punish, jail, or limit the liberties of citizens in ways that corporations don't. For example, the severity of an invasive behavioral ad from a company may pale when compared with the severity of being jailed by the government or being denied a travel visa. Furthermore, such harms may be more easily envisioned than more abstract risks of corporations' data use, such as profiling or data aggregation.

Previous incursions on privacy and liberties imposed by the U.S. government, such as internment camps [8], and surveillance of civil rights leaders [9] may be more salient to some citizens than others. Many, including the author, are concerned that the possibility of abuse of power and miscarriage of justice in the U.S. has not been fully eliminated.

Therefore, the difference in control and severity of risk can change how people perceive the government using their data versus corporations using the same data. This ability to imagine and dread government's power may hold even if the person has done nothing wrong.

WHAT'S THE HARM?

How people perceive the risk can change their behavior; they may deliberately restrict their own speech or social network activities. Regardless of the actual probability of harm, perceptions of harm from government use of data can create a chilling effect.

People who believe they are being watched may act differently and may be less likely to express themselves online, or they may withhold ideas that they believe are not dominant [10]. The perception – even incorrect – that objective harms could come from government use of data can further exacerbate this chilling effect on free speech.

Free speech is not the only social value that individuals might voluntarily curb due to perceived government surveillance and risks. Freedom of association and religion may also be impacted if one perceives that there is government surveillance. Therefore, governments have an extra burden to reduce the perception of risk from use of social network data.

SOCIAL GOOD VERSUS PRIVACY HARM

At the same time, government agencies are frequently engaged in public policy decisions, with the objective of providing benefits to society. As such, public policy decisions may differ from those made by corporations, or even researchers. Ideally, a government agency should provide services for the public good, even when it is not profitable. Given that there are privacy risks from government use of social network data, the natural question is whether the social good from using the data outweighs the privacy risks.

We think this is the right question to ask. However, we highlight many unsolved issues in getting to the answer. How does one measure social good? What metrics should be used? Traditional metrics, such as putting a dollar value on costs or benefits or privacy or health, may be either unavailable or inappropriate. What if those data contain information that is demonstrably and unequivocally relevant to the public welfare? How much can we trade the public welfare for privacy?

Pareto optimality is a state that public policy makers may wish to strive for in their decision making, as it implies that resources (and risk) are distributed in the most efficient way. It remains unclear whether that is achievable, and even how it can be measured. Without serious uncertainty analysis, so-called optimal solutions will often be poor choices.

CONCLUSION

Some may argue that privacy concerns with government use of social media data are minimal because the government has checks and balances, or that data is public. We reject these arguments since privacy harms can still occur, resulting in a chilling effect, and that the distinction between public and private data is a false dichotomy. In this paper, we have argued that government agencies engaged in using social media data cannot ignore privacy concerns, and indeed have an additional responsibility to address perceptions of risk. This requires not only best practices in protecting the data, but also improved communication, transparency, and notice about the data use.

A government agency who wishes to use social media data may try to reduce the perception of harm through education. Explaining what the government is doing with social network data is necessary, but may be a complicated problem. Meaningful notice about data use can be difficult [11]. Furthermore, an ethical U.S. government agency would need to explain the data use across the spectrum of education levels and languages in the United States.

If a U.S. government agency is considering the use of social media data, we argue that the correct issue to be resolved is how to weigh privacy harms with social goods. This is a thorny problem, in which both the metrics or the methods for analysis are unsettled and may have large uncertainties, but we encourage government agencies to consider this type of analysis before engaging in social media use. The National Institute of Standards and Technology has recently published guidance for assessing privacy risks [12], which we see as a valuable contribution to this conversation.

Although we use social network data to provide a specific context, we believe that these arguments could apply to data from other sources. This could include search engine terms, location data, or other data from websites, smartphone apps, or sensors.

This paper has focused on U.S. government data of citizen data, and we have given U.S.-specific examples. We believe that findings from the field of risk perception will be applicable to similar discussions in other countries. However, the specific perceptions of how governments could use (or abuse) private data may differ in other countries, cultures, and legal regimes.

REFERENCES

[1] A. Wesolowski, N. Eagle, A. J. Tatem, D. L. Smith, N. A. M., R. W. Snow and C. O. Buckee, "Quantifying the Impact of Human Mobility on Malaria," *Science,* vol. 338, no. 6104,

pp. 267-270, 12 Oct 2012.

[2] R. Nixon, "Visitors to the U.S. May Be Asked for Social Media Information," NyTimes.com, 28 June 2016. [Online]. Available: http://www.nytimes.com/2016/06/29/us/homeland-security-social-media-border-protection.html. [Accessed 12 Dec 2016].

[3] E. Bodine-Baron, T. C. Helmus, M. Magnuson and Z. Winkelman, "Examining ISIS Support and Opposition Networks on Twitter," RAND Corporation, Santa Monica, 2016.

[4] H. Nissenbaum, "Privacy as contextual integrity," *Washington Law Review,* no. 79, p. 119, 2004.

[5] M. Kosinski, D. Stillwell and T. Graepel, "Private traits and attributes are predictable from digital records of human behavior," *PNAS,* vol. 110, no. 15, 9 April 2013.

[6] R. Calo, "The Boundaries of Privacy Harm," *Ind. LJ,* vol. 86, p. 1131, 2011.

[7] P. Slovic, B. Fischhoff and S. Lichtenstein, "Facts and fears: Understanding perceived risk," *Societal risk assessment,* pp. 181-216, 1980.

[8] M. Conrat and R. Conrat, Executive Order 9066: The Internment of 110,000 Japanese Americans., 1972.

[9] D. J. Garrow, The FBI and Martin Luther King, Jr.: From" Solo" to Memphis, Open Road Media.

[10] P. E. N. America , "Chilling Effects: NSA Surveillance Drives US Writers to Self-Censor," New York: PEN American Center, 2013.

[11] L. F. Cranor, "Necessary but not sufficient: Standardized mechanisms for privacy notice and choice," . *on Telecomm. & High Tech. L,* no. 10, p. 273, 2012.

[12] S. Brooks, M. Garcia, N. Lefkovitz, S. Lightman and E. Nadeau, "An Introduction to Privacy Engineering and Risk Management in Federal Systems," 1 January 2017. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf. [Accessed 29 January 2017].