This document was produced based on notes taken during the Social Media Surveillance and Law Enforcement workshop of the Data & Civil Rights conference. This document represents a general summary of the discussion that took place. Not all attendees were involved in every part of the conversation, nor does this document necessarily reflect the views and beliefs of individual attendees. All workshop participants received workshop materials prior to the event to spark discussion. The primer can be found at: http://www.datacivilrights.org/pubs/2015-1027/Social_Media_Surveillance_and_Law_Enforcement.pdf

Workshop Discussion Notes: Social Media Surveillance and Law Enforcement

Overview

This workshop gathered individuals drawn from law enforcement, social justice movements, technology companies, academia and government to discuss the effects of social media surveillance by law enforcement. The conversation was grounded in concerns over how social media surveillance may reproduce existing policing practices that disproportionately target people of color, marginalized populations, and activists. With an acknowledgement that people's expectations to privacy are not as clear in the online world as they are on the ground, participants grappled with how protections of free speech and privacy must adapt to social media.

The first session focused on addressing the questions, how do communities use social media, and how closely does social media reflect reality? How are threats on social media identified by law enforcement, and what biases may exist in where these threats are sought out? The second session addressed how social media companies increasingly play an intermediary role between their users and law enforcement. What responsibility do companies have to mitigate social justice issues, and what are their limits? The discussion also touched upon questions of algorithmic design and the ways in which bias and discrimination can be embedded in surveillance technologies. The workshop concluded with a discussion on what kinds of policies and legal interventions could be made to ensure greater transparency and accountability from law enforcement, social media companies, and technology vendors.

Themes and discussion topics

Challenges in interpretation

The workshop began by considering how activity on social media can easily be misinterpreted out of context, and can present a distorted reflection of people's lives. When a person's Tweets and Facebook posts become evidence in criminal investigations and feed into risk assessments, misinterpretation based

on, for example, contextual misunderstandings can have serious consequences. As a result, what kinds of trainings, policies, and expertise could aid law enforcement in better assessing social media in an investigative context? Participants underscored that language is intrinsically complex. For example, a person may post on social media in a way that performatively alludes to criminal activity, but may not necessarily reflect realities on the ground. A recurring point through the workshop was a fear that current practices of heightened surveillance of communities of color are being reproduced online. As a result, what kinds of expertise and actors are needed to ensure that individuals are not unfairly criminalized based on their social media activity?

Some participants proposed that police officers who are strongly embedded in communities are best able to interpret online speech. Others disagreed, noting existing policing practices that are fraught with misreadings of behavior. For example, some state-wide gang databases have only a small number of criteria, where factors like age, social associations, and clothing choices can be enough to place an individual in a gang database. Such practices can blur the lines between intelligence-gathering and stereotyping, and can have long-lasting effects when records are kept for decades or more. Another difficulty for gang databases has been that often there is inadequate staffing to oversee accurate data entry when funding dries up, which can have serious consequences when prosecutors rely on that data to make arrests and charge individuals with crimes. There was a concern that the same problems of accountability, accuracy, and stereotyping may arise with new technologies that allow police to monitor online activity on a larger scale.

What counts as a threat?

The discussion then turned to examining the limits of social media surveillance more generally. Participants pointed out that the concept of risk is not neutral -- where law enforcement seeks out criminal behavior is a function of what it will find. What kinds of online behavior are flagged as a threat, whether by manual or by automated means? Among which populations in particular is law enforcement seeking out determinants of risk? Are there ways to create and make use of generalizable assessments of risk? Issues of accountability are raised when considering what kinds of expertise should be present when deciding what constitutes a threat, and it was underscored that greater diversity and a wider range of stakeholders are needed.

Recalling the earlier discussion on interpretation, the example of Black youth being targeted for writing anti-police posts on social media was brought forward. Where can the line be drawn between identifying legitimate threats, and profiling? One discussant noted how the online activities of white supremacist groups are often subject to less scrutiny, and there have been instances where online threats to commit violence are only discovered by law enforcement and the media after an act of violence, such as a mass shooting, has been perpetrated. Where funding and resources for surveillance are being allocated, and whether they are allocated fairly, needs to be considered a civil rights issue alongside the protection of free speech and privacy.

The practice of monitoring the online activities of activist and protest movements was also brought into question. The group agreed that the rise of social media has altered the dynamics of free speech in both positive and detrimental ways -- facilitating new avenues for organizing movements and amplifying voices, but also exposing them to greater scrutiny. Many of the activists and organizers in the room related their personal experiences with police surveillance, including being approached and identified by officers on the street by their Twitter handles. The potential chilling effects of surveillance were brought up, and one organizer explained how awareness of police surveillance has compelled them to move activities, such as protest planning, off of social media.

Law enforcement and the private sector

The remainder of the workshop focused on the intersection between law enforcement and the private sector, including social media platforms, surveillance vendors, and potential third party organizations that might be able to advocate on behalf of citizens. Social media companies play a role in arbitrating which search warrant requests to challenge and, unless there is a gag order, they have the power to inform users when law enforcement is requesting access to their private communications. However, it was countered that platforms often receive very little information with requests, and in most cases have little legal standing to challenge them. They are also not necessarily well-equipped to interpret and contextualize legitimate threats from illegitimate ones. These issues raised the question, to what extent can and should social media companies act as gatekeepers against police access to private communications?

Another concern raised is that many people are generally not well-positioned to challenge law enforcement when they become the target of surveillance -- very often they are not aware that they are being surveilled, and may not have the money or resources to contest law enforcement in court. Given that platforms cannot provide legal counsel for their users, the group considered other avenues, such as an entity or organization, along the model of the Electronic Frontier Foundation, that could advocate on behalf of social media users. Ensuring greater digital literacy and more easily consumable information on users' privacy rights were also discussed as priorities. However, some disagreed, pointing out that users, particularly young people, are unlikely to behave more cautiously on social media, even if they are better informed about their privacy rights. A lingering question was, whose responsibility is it to ensure the literacy of users?

In addition to social media companies, technology vendors are also playing a greater role in how law enforcement gather intelligence online. With an entire industry arising around the technological identification of online triggers, the design decisions of surveillance vendors also have implications for civil rights. One participant explained how, in designing algorithms, it is often the case that datasets do not have adequate representation of minority groups, to the point where machine learning algorithms will sacrifice accuracy for these groups for the sake of higher overall accuracy. This can have unfair or discriminatory consequences down the line, which underscores the need for better datasets. Further compounding this effect is the fact that designers often do not work closely with the populations whom

those algorithms most closely affect. And many actors who deploy algorithms, both in law enforcement and criminal justice more broadly, lack a deep understanding of how they work.

Accountability and transparency

The workshop closed with a discussion on ways to move forward, asking what kinds of mechanisms can be put in place in the future to ensure greater transparency and accountability. To launch the conversation, a law enforcement representative recounted his department's experience in developing a policy to govern the use of social media. While the policy was based around legal requirements and Fourth Amendment rights, he also noted that understandings of privacy have changed in the age of social media, which poses a challenge in reconciling expectations to privacy that are not necessarily recognized by the law. On the issue of transparency, he noted that practices such as deciding what kinds of intelligence gained from social media is actionable, and how information is collected and stored are all processes that need to be documented. Another participant called for departments to make these policies easily accessible to the public, such as uploading them online. Other policy issues came up in the discussion, such as tensions between law enforcement strategies and social media company policies. For example, the police use of fake social media accounts to engage in undercover operations is in fact prohibited by some social media platforms according to their Terms of Service. The discussion coalesced around how law enforcement policy can better regulate practices, and whether policies can be generalized across departments.

A gap in knowledge about police surveillance of social media was cited as a major obstacle for accountability. In addition to a lack of transparency in local law enforcement, there is also little public understanding of how online surveillance is occurring on a national level, through agencies like the FBI, NSA, and DHS that share intelligence at fusion centers. On the level of targeted surveillance, there is inadequate information on who is being surveilled, and where biased or disproportionate targeting is occurring on a larger scale. It was suggested that social media companies can use the data they have to note disparities and trends, such as patterns of subpoenas they receive, or other categories that the public would find of interest. Another participant noted the potential to use data to identify specific police departments that are making disproportionate numbers of subpoenas to social media companies for private communications.

Finally, the responsibilities of technology vendors for their design decisions were also noted. There was a general sense that software had positive potential, but there was also a concern that it paved the way for new forms of surveillance, while posing challenges for identifying bias. One of the implications of surveillance technology is that it introduces multiple layers where bias can creep in. For example, officers may rely on risk assessments based on social media data while being left in the dark with regards to the underlying data points.

Areas for Further Exploration

An ongoing theme of the workshop was determining where the onus of responsibility lies for mitigating the threats posed to civil rights, free speech, and rights to privacy by online surveillance. On the one hand, there was disagreement over whether any burdens should be placed on users of social media. Is better digital literacy needed? Should people be more cautious about what they post online? On the other hand, it was broadly agreed that police departments must take steps to develop clear policies and procedures, and to make them available to the public. By virtue of their role as platforms, social media companies occupy a central but uncertain position -- they can limit the ways they get involved in surveillance practices, but in many ways they are already implicated through the design decisions they make, such as default privacy settings, and the ways they handle police requests for private communications. To what extent should social media companies involve themselves in negotiating the limits of police surveillance? With regards to surveillance technology, what kinds of accountability mechanisms can be put in place to test bias? The overall conclusion was a need for greater diversity of expertise in influencing designers of surveillance tools, as well as taking into account the lived experiences of marginalized populations that historically have faced the brunt of police surveillance.