Why Police Should Monitor Social Media to Prevent Crime

Christopher Raleigh Bousquet, *Wired*, 20 April 2018 (adapted)

In February, the ACLU[1] of Massachusetts released a report revealing that between 2014 and 2016, the Boston Police Department (BPD) had tracked keywords on Facebook and Twitter in an effort to identify potential terrorist threats. The BPD labeled as "Islamist extremist terminology" keywords like "ISIS" and "Islamic State," but also phrases like "MuslimLivesMatter" and "ummah," the Arabic word for community. A 2016 report from the ACLU of California revealed that cities were targetting words like "#blacklivesmatter" and "police brutality" following the killings of Michael Brown and Freddie Grey.

These practices by the BPD reflect a growing trend in law enforcement called social media mining. Using natural language processing tools, police departments scan social platforms for keywords they believe indicate danger. A 2016 survey by the International Association of Chiefs of Police and Urban Institute revealed that 76 percent of officers use social media to gain tips on crime, 72 percent to monitor public sentiment, and 70 percent for intelligence gathering.

Police departments should continue to monitor social media to inform law enforcement. After all, social media sites are full of data that can make police interventions more effective, from posts about crimes in progress to damning evidence offered freely by criminals and even live videos of crimes.

Do citizens have a reasonable expectation of privacy regarding social media posts? One might think that because this information may be publicly available to anyone on the internet, users would abandon any privacy expectations when posting, liking a page, or checking into a location. And yet, very few users expect someone to track every single piece of their social media activity over the course of a week, month, year, or longer—as police departments often do with social mining.

The other issue that social mining raises is free speech. The ACLU has argued that the practice has a chilling effect, discouraging free expression.

Yet just because social mining has a chilling effect does not mean that it's unconstitutional. If a practice like social media mining effectively addresses an important policy goal—reducing violent crime, for instance—it is Constitutionally acceptable even if it restricts speech.

Christopher Raleigh Bousquet (@chrisrbousquet) is a researcher at the Ash Center for Democratic Governance and Innovation, a think tank out of Harvard Kennedy School.

[1] the American Civil Liberties Union, a major nonprofit organisation.

Without encryption, we will lose all privacy. This is our new battleground

Edward Snowden, *The Guardian*, 15 October 2019 (shortened)

In every country of the world, the security of computers keeps the lights on, the shelves stocked, the dams closed, and transportation running. For more than half a decade, the vulnerability of our computers and computer networks has been ranked the number one risk in the US Intelligence Community's Worldwide Threat Assessment—that's higher than terrorism, higher than war.

And yet, in the midst of the greatest computer security crisis in history, the US government, along with the governments of the UK and Australia, is attempting to undermine the only method that currently exists for reliably protecting the world's information: encryption. Should they succeed in their quest to undermine encryption, our public infrastructure and private lives will be rendered permanently unsafe.

Earlier this month the US, alongside the UK and Australia, called on Facebook to create a "backdoor", or fatal flaw, into its encrypted messaging apps, which would allow anyone with the key to that backdoor unlimited access to private communications. So far, Facebook has resisted this.

If internet traffic is unencrypted, any government, company, or criminal that happens to notice it can—and, in fact, does—steal a copy of it, secretly recording your information for ever.

I know a little about this, because for a time I operated part of the US National Security Agency's global system of mass surveillance. In June 2013 I worked with journalists to reveal that system to a scandalised world. Without encryption I could not have written the story of how it all happened—my book *Permanent Record*—and got the manuscript safely across borders that I myself can't cross. More importantly, encryption helps everyone from reporters, dissidents, activists, NGO workers and whistleblowers, to doctors, lawyers and politicians, to do their work—not just in the world's most dangerous and repressive countries, but in every single country.

To justify its opposition to encryption, the US government has, as is traditional, invoked the spectre of the web's darkest forces. Without total access to the complete history of every person's activity on Facebook, the government claims it would be unable to investigate terrorists, drug dealers, money launderers and the perpetrators of child abuse—bad actors who, in reality, prefer not to plan their crimes on public platforms, especially not on US-based ones that employ some of the most sophisticated automatic filters and reporting methods available.