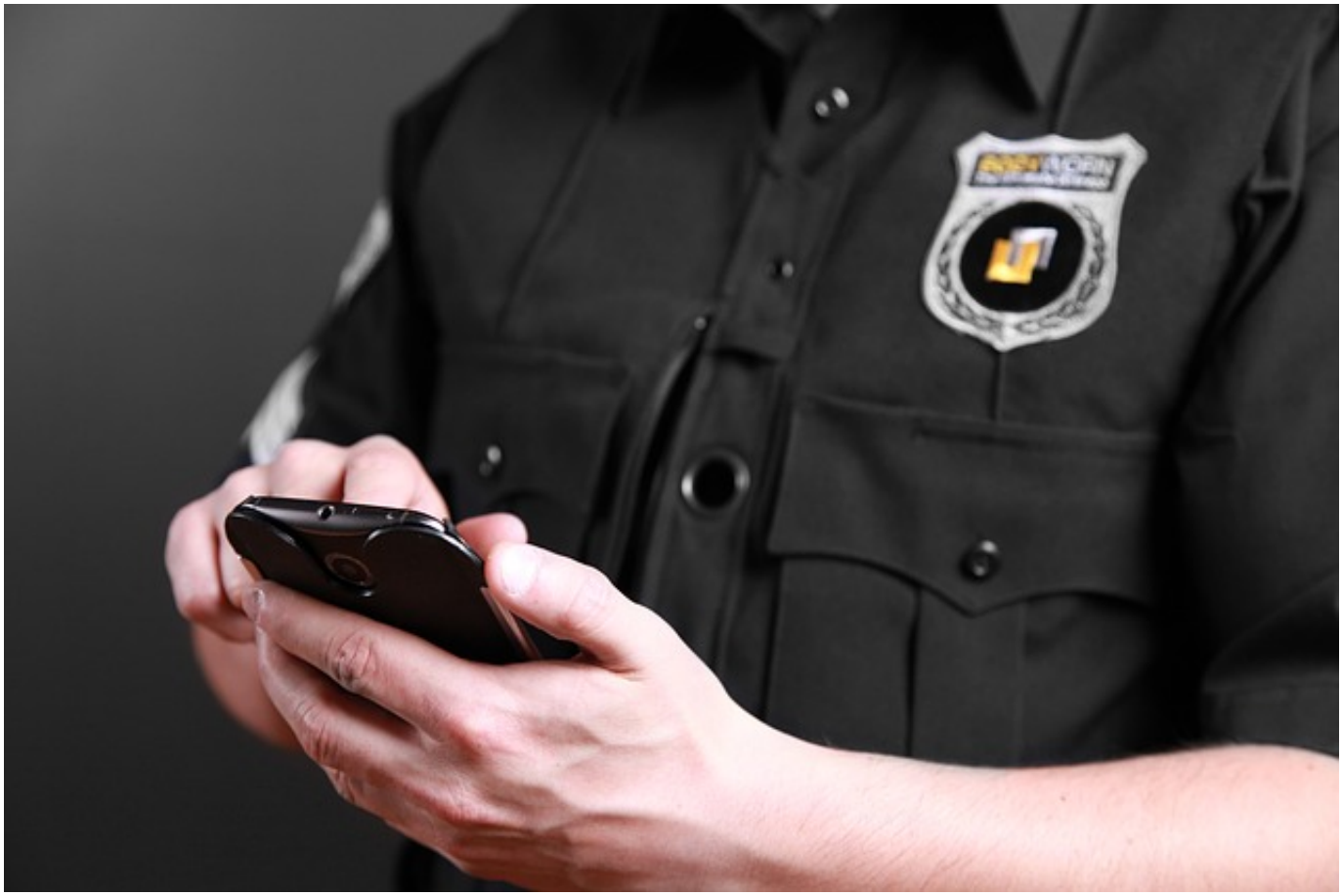
Participation, Trust and Location-Based Social Media Government Monitoring

Author : John Stephens

Categories : Online Participation, Public Meetings

Tagged as : Government Social Media; geolocation; monitoring social media; Facebook; Geofeedia; SeeClickFix; Open Town Hall; Next Door; crowd management; public rallies; privacy

Date : August 28, 2015



Social media is a growing part of the civic engagement landscape. We'll describe how local government, especially law enforcement, could be using it in ways that pose some risk of undermining the trust and effectiveness of online methods for citizen participation.

> *Imagine this scene: Your 15-year-old daughter is at a local music festival, Carolinaville Lollapalooza . She's using Instagram and there's a 'selfie' of her having fun with two*

> *young guys. You are following her instagram, so you're a bit uncomfortable. The next picture has one of the guys with a bottle - it looks like beer - and all three of them being even more friendly. You hope she knows when to stop. A minute later, there's a picture of a police officer and your daughter. Is she being arrested? What's going on?*

If public safety officials are monitoring all the Instagram feeds tagged #CarolinavilleLollapalooza, and they are using geolocation to hunt for suspicious behavior - including underage drinking - this could be the outcome of your daughter's sharing her fun with her "new friends."

This may seem like a far-fetched idea, but the technology is already here, and social media is raising issues about privacy, consent, and government monitoring.

For strong civic engagement, there need to be safe ways to speak out and protections from government officials poking around to "find you" for no good reason.

Social Media and Geolocation

Geolocation is just one of many common tools, and we all use it every day without really thinking about it: finding a good restaurant, getting directions, attending a meeting that's in our online calendar, or finding friends and social groups.

When it comes to government, the feeling can be very different. No one wants "Big Brother" monitoring where they are: that is an invasion of privacy. At the same time, we can acknowledge certain appropriate uses, and not just dramatic examples of tracking suspected terrorists.

We summarize the capabilities, advantages and concerns related to geolocation monitoring of social media networks designed for public safety, fire, police, and other emergency management departments.

Finding folks on social media - how it works

There are various options to find the physical location of a social media user. (If you're interested in seeing just how many, check out this article.). There's a good write-up of Geofeedia, one of the first social media monitoring tools, on the SOG's Community Engagement Blog here.

When you use social media, you allow companies to geolocate your posts, photos, shares, tweets, and check-ins based on your device's GPS location. Social media monitoring tools [software] then allow users to specify a geographic region, state, zip code, country, or area of interest from which

they pull location data from users on social media to show real-time posts.

Geolocation monitoring was initially developed by the private sector - companies wanted to be able to see, for example, what stores a person chose in a large mall and what purchases they made. Only in the last ten years - for a variety of reasons - did the public sector begin to tap into geolocated data. Examples include SeeClickFix, Open Town Hall, and NextDoor. These and other social media apps require physical address verification for participation in public forums online.

Legitimate uses of "tracking people" via social media geolocation

We can imagine several appropriate - and probably widely acceptable - uses by public safety officials of this kind of technology:

1. Using drones for seeking missing hikers based on their geolocated posts
2. Performing crisis management, such as when there is an active shooter scenario and law enforcement can visually track posts to see the location of hostages and/or perpetrators
3. Managing disasters, so that first responders can find the location of fallen trees, flooding, or people in need of assistance.

Crowd and protest management: issues of safety and privacy

However, there's at least one more purpose that begins to blur the line between safety and privacy: the use of geolocated social media in crowd management.

There's an obvious public safety component when large groups of people gather for any purpose, especially rallies and protests: tensions are higher, the potential for damage is greater, and it's harder to monitor suspicious activity.

Does it matter if those groups are gathered for #CarolinavilleLollapalooza or a protest in Ferguson, Missouri? Is there, or should there be, a different approach to those two large groups gathering?

Social media has been demonstrated to have a significant impact on cultural and social change movements - the Arab Spring is probably the best example, with movements fueled by Facebook and Twitter, used to connect people on the ground and share their story with the broader world. Some are even suggesting that without those forms of public protest and citizen journalism, the events in Ferguson would have never made it onto the national stage.

How does this type of geolocation monitoring prevent or inhibit those tools from serving

legitimate purposes for the greater good?

John

Consider these three situations of government using geotagging to know where you are. I label them as legitimate, illegitimate and grey zone, but you may see them differently.

- Legitimate: Lost child in the woods or “silver alert” for a disoriented senior who is lost. It’s always best for a parent or guardian to request police help before the active social media seeking begins. This situation of risk of harm and government action seems an easy case for using geolocation technology.
- Illegitimate: Public safety, social services, or other officials keeping a database of geotag identities and movements. Lacking a rationale for protection or public order, this seems a clear invasion of privacy and the worst “big brother” fears - they always know where you are (as long as your smartphone or Apple watch is on).
- Grey zone: Monitoring of a crowd at a public event; concerns for public order and small-scale law violation. The opening scenario, about underage drinking, illustrates this problematic use.

Emily

Even if you think you’ve changed your privacy settings to avoid geolocating your posts, it may be worth a closer look. Often, large tech companies, such as Facebook and Google, only allow you to change settings for certain elements of their privacy policies - retaining company control over certain data.

Consider the recent story about the real-world Marauder’s Map, created by a 23-year-old Harvard student intern at Facebook earlier this year. Aran Khanna discovered soon after he started at the company that even when users had turned off geolocation monitoring on their posts and photos, it was automatically being used for private messages. Any message sent or received on Facebook could identify the user and locate their device - to within a meter of where they were - whether or not they were already friends or not.

> *Imagine this for your theoretical 15-year-old: her friends copy her into a group message on Facebook that includes a 26-year-old registered sex offender. They aren’t connected on Facebook and your daughter has done nothing wrong...but her location, to within three feet, is now available to everyone on that list, and she’s walking home alone from school today.*

Khanna created the Marauder’s Map plug-in to highlight that discrepancy at Facebook, and it was downloaded 85,000 times before Facebook responded and asked him to remove it. He was fired from his internship, and Facebook still has not issued a public response or update to address these privacy issues.

Emily and John

We seek your thoughts on these civic engagement questions:

1. Should government be barred from using geolocation apps for all rallies and protests as long as they are peaceful?
2. Should police be permitted to use geolocation for suspected minor offenses - such as underage drinking?
3. Should Facebook and other social media businesses be required to show users that they are being geolocated - and give users the power to turn it off entirely?