Journal of Business & Technology Law

Volume 12 | Issue 2 Article 2

Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space

Jeramie D. Scott

Jeramie D. Scott*

Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space

I. INTRODUCTION

Social media sites are public space and government mass surveillance of this public space undermines our democracy. As we spend more and more of our lives on digital mediums, the government is monitoring publicly available social media data more than ever.[1] At the same time, the Internet, particularly social media, has become an important public space to exercise First Amendment rights.

Roughly two-thirds of Americans use social media accounts.[2] People use social media to share ideas, explore new ideas, and engage those with similar and dissimilar ideas. Additionally, social media has become a key tool of social movements like the Occupy Movement and Black Lives Matter.[3]

This Essay will examine the government's use of social media monitoring services to collect, monitor, and analyze social media data for the purposes of fighting crime and terrorism. After explaining the use of social media monitoring,[4] I will examine the importance of "privacy in public."[5] Following, I will discuss the dangers of this monitoring and the lack of legal protection.[6] In conclusion, I will offer the necessary actions that must be taken to protect our privacy and ultimately our First Amendment rights in an age of social media monitoring.[7]

* EPIC's National Security Counsel and Director of EPIC's Domestic Surveillance Project.

1. *Map: Social Media Monitoring by Police Departments, Cities, and Counties*, Brennan Center for Justice (Nov. 16, 2016) [hereinafter *Brennan Center Map*], https://www.brennancenter.org/analysis/map-social-media-monitoring-police-departments-cities-and-counties.

2. Shea Bennett, *67% of Americans Use Social Media (With One in Six Active on Twitter)*, Ad Week: Social Times (Apr. 2, 2014), http://www.adweek.com/socialtimes/social-media-america/497615.

3. *See, e.g.*, Bijan Stephen, *Social Media Helps Black Lives Matter Fight the Power*, Wired Mag. (Nov. 2015), https://www.wired.com/2015/10/how-black-lives-matter-uses-social-media-to-fight-the-power.

4. *See infra* Part II.

5. *See infra* Part III.

6. *See infra* Parts IV–V.

7. *See infra* Part VI.

II. SOCIAL MEDIA MONITORING SOFTWARE

With the rise of social media, many companies now provide social media monitoring software that the government can use to sift through the vast amount of data created by social media. Digital Stakeout,[8] Beware,[9] Geofeedia,[10] LifeRaft[11] are just some of the names of the products provided for monitoring social media. These products are used by the federal government as well as local and state governments to aggregate, filter, and analyze billions of data points created across social media platforms every day.[12] Even the Central Intelligence Agency's venture capital firm, IN-Q-TEL, is investing heavily in companies that are working on software tools to mine the vast amount of social media data.[13]

Social media monitoring software is used in a variety of ways to analyze the "big data" derived from collecting social media information. The software is not just used to look for keywords,[14] but also to track the location from which social media posts are coming,[15] identify relationships between people,[16] monitor events,[17] and determine an individual's potential for violence,[18] among many other functions.

The social media monitoring software known as Beware has been used by the Fresno, California police to data mine publicly available records, including social media, to produce "threat scores" that predict "the suspect's potential for violence."[19] Threat scores are color-coded as green, yellow, or red with red being the highest threat.[20]

8. DIGITALSTAKEOUT, http://www.digitalstakeout.com (last visited Feb. 1, 2017).

9. *Beware*, WEST, https://www.west.com/safety-services/public-safety/powerdata/beware (last visited Feb. 15, 2017).

10. GEOFEEDIA, https://geofeedia.com (last visited Feb. 15, 2017).

11. LIFERAFT, http://liferaftinc.com (last visited Feb. 15, 2017).

12. *See Brennan Center Map*, *supra* note 1.

13. Lee Fang, *The CIA is Investing in Firms that Mine Your Tweets and Instagram Photos*, THE INTERCEPT (Apr. 14, 2016), https://theintercept.com/2016/04/14/in-undisclosed-cia-investments-social-media-mining-looms-large.

14. *See generally Features*, SIGNAL, http://www.getsignal.info/features (last visited Feb. 15, 2017).

15. *Id*.

16. *Corporate Security,* LIFERAFT http://liferaftinc.com/Solutions/Corporate-Intel (last visited Mar. 2, 2017).

17. Nate Anderson, *How the Cops Watch Your Tweet in Real-Time*, ARS TECHNICA (Sep. 15 2013), https://arstechnica.com/tech-policy/2013/09/how-the-cops-watch-your-tweets-in-real-time (explaining how the Bluejay program allows police to monitor and locate, in real-time, public tweets).

18. *See Beware*, *supra* note 9.

19. Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat "Score,"* WASH. POST (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html.

20. *Id.*

A number of law enforcement authorities have tracked the Black Lives Matter movement through social media monitoring. Authorities in Oregon used social media monitoring software to track Black Lives Matter hashtags.[21] The Department of Homeland Security ("DHS") has collected information about the movement from various social media accounts including Facebook and Twitter.[22] Mall of America Security scraped information from social media accounts to build dossiers on Black Lives Matter activists.[23]

Social media monitoring software ingests a vast amount of data from a number of different types of accounts, including Facebook, Twitter, Instagram, YouTube, Google+, Foursquare, Reddit, Vine, Tumblr, Periscope, and several others.[24] Geofeedia is a location focused monitoring software that, according to its website, helps "[d]iscover trends and patterns within the world's largest set of location-based social data to inform better decision-making."[25] Bluejay markets itself as a "Twitter crime scanner" that allows the user to monitor high profile events.[26]

This rise in social media monitoring allows law enforcement to now conduct a "virtual stakeout" of everything happening in the public space of social media. This level of surveillance is chilling and undermines our First Amendment protected rights and compromises our democracy. The public availability of so much data requires us to rethink privacy in public and implement the protections necessary to preserve our freedoms.

III. IMPORTANCE OF PRIVACY IN PUBLIC

The concept of "privacy in public" can seem like an oxymoron at first glance, but the concept is absolutely essential in a well-functioning democracy. Privacy in public allows for self-realization;[27] supports the freedom of thought[28] and associational rights;[29] and prevents conformity of thought and the chilling of

21. *Id.*

22. George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, THE INTERCEPT (July 24, 2015), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson.

23. Lee Fang, *Mall of America Security Catfished Black Lives Matter Activists, Documents Show*, THE INTERCEPT (Mar. 18, 2015), https://theintercept.com/2015/03/18/mall-americas-intelligence-analyst-catfished-black-lives-matter-activists-collect-information.

24. *See, e.g.*, DIGITALSTAKEOUT *supra* note 8.

25. GEOFEEDIA, *supra* note 10.

26. Anderson, *supra* note 17.

27. *See* Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26, 37 (1976) ("I shall myself argue that the right to privacy is fundamentally connected to personhood.").

28. *Id.* at 39.

29. *Id.*

speech,[30] thus protecting the "free market of ideas" that is vital for proper democratic discourse.

Traditional theories of privacy have focused on "securing intimate and personal realms."[31] The focus was on actual threats to privacy.[32] Not until the rise of information technology and databases was there a perceived threat to privacy in public.[33] Privacy in public was traditionally protected by economic and technological limitations that made public information largely obscure.

In an age before information technology, it would have been extremely hard to collect, analyze, and retain large amounts of public information over a long period of time of just one person, let alone millions. Aggregating disparate public records and surveilling the public activities of one individual would take a great deal of manpower. The practical obscurity of public information meant large scale surveillance of the public was a minimal concern at best, but the loss of this obscurity has made indiscriminate mass surveillance an everyday occurrence.

This idea of privacy through obscurity has been applied to the online realm. Woodrow Hartzog and Frederick Stutzman proposed determining online obscurity based on four factors: search visibility, unprotected access, identification, and clarity.[34] In the Hartzog/Stutzman framework, the presence of these factors decreases any claim to obscurity.[35] Accordingly, the absence of these factors increases obscurity.[36] This framework for obscurity, and others, tend to leave no room to protect the privacy in public of online data, (e.g. social media posts) that are widely available and lack some element restricting the information or the identity of the poster from the public. Joel Reidenberg has used obscurity as a starting point to understand the loss of privacy in public.

Reidenberg describes this loss of practical obscurity in three stages: (1) obscurity, (2) accessibility, and (3) transparency.[37] The obscurity stage precedes mass deployment of information technologies and preserves privacy in public through the sheer difficulty and cost of more traditional surveillance (i.e. surveillance that requires significant manpower).[38] The accessibility stage implements the technology that makes personal information accessible to the public.[39] Think of the ubiquity of

30. *Id.*

31. *See* Helen Nissenbaum, *Toward an Approach to Privacy in Public: Challenges of Information Technology*, 7 ETHICS & BEHAV. 207, 207 (1997).

32. *Id.*

33. *See* Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141, 142 (2014).

34. Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 35–40 (2013).

35. *Id.* at 4.

36. *Id.*

37. Reidenberg, *supra* note 33.

38. *Id.* at 148.

39. *Id.* at 148–49.

cameras from CCTV to cellphones in everyone's hands that can take pictures and record video. The digitization of public records would be another example. The transparency stage takes all this newly accessible information and makes it conspicuous through technologies like search engines or social media sites.

It is social media that often exposes us to all the information that is now readily accessible, thus making it transparent. An enormous number of pictures and video are posted on sites like Facebook, Instagram, YouTube, and other social media sites. These social media posts expose what was once completely obscure and inaccessible. But, social media monitoring is arguably an example of a fourth stage to Reidenberg's loss of practical obscurity— "analysis."[40]

Beyond removing the obscurity to public information and making it accessible and transparent, social media monitoring takes that information and analyzes it to derive additional informational value from the large amount of personal information that is now available.

In the age of mass social media monitoring, our concept of obscurity and privacy in public needs to expand. Privacy in public is vital to our democracy. In the context of the online public spaces created by social media, I do not intend for privacy in public to mean the restriction of access to posted material. Additionally, I do not intend for privacy in public to mean some level of purposeful obscurity by the individual posting on social media. The privacy in public for social media I am advocating means there is no government-coordinated mass surveillance to indiscriminately analyze and assess all social media including what was said, who said it, and the associations of the social media poster in an attempt to draw conclusions about the speaker regarding criminal or national security threats. We must allow the space for social media users and posts to enjoy a sort of practical obscurity obtained by the sheer volume of social media data available. It is this practical obscurity that will allow the "market place of ideas" to thrive in our digital world.

Where we allow our digital public spaces, i.e. social media, to become bastions of mass surveillance we will see a slow degrade of public discourse. Indeed, to a certain extent, we have already seen that. Since the Snowden revelations, more and more individuals have either taken steps to shield their online information from the government or self-censored what they discuss in online public forums. A Pew survey found that 34% of adults who have become aware of the surveillance programs have taken steps to shield their information from the government.[41] This

40. *See* Jouvenal, *supra* note 19 (using social media monitoring program to analyze "billions of data points, including arrest reports, property records, commercial databases, deep Web searches and [a] man's social- media postings" to calculate a suspect's threat level).

41. Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RESEARCH CENTER (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden.

includes changing social media privacy settings, using social media less, and avoiding certain terms in online communications.[42]

A report by PEN America, which surveyed nearly 800 writers around the world about surveillance and self-censorship, found that:

> *Writers living in liberal democratic countries have begun to engage in self-censorship at levels approaching those seen in non-democratic countries, indicating that mass surveillance has badly shaken writers' faith that democratic governments will respect their rights to privacy and freedom of expression, and that—because of pervasive surveillance—writers are concerned that expressing certain views even privately or researching certain topics may lead to negative consequences.*[43]

The PEN America report also found that over 1/3 of writers hailing from free countries outside the U.S. thought that freedom of expression was less protected in the U.S. compared to their own country.[44] Additionally, large portions of the writers surveyed have limited their social media activities or avoided social media altogether.[45]

As social media monitoring increases and becomes more sophisticated and the mass surveillance of public spaces increases, it will have a detrimental impact on our democracy.

IV. SOCIAL MEDIA MONITORING: A LURKING DANGER FOR OUR SOCIETY

The mass surveillance and analysis of publicly available data, particularly social media data, has far reaching implications for society. Social media monitoring threatens to limit our associations, chill our speech, and generally target those engaged in First Amendment protected activities.

The implications of social media monitoring are particularly dangerous for minorities and those who express unpopular views. The capabilities of social media monitoring have already been directed towards the Black Lives Matter movement.[46] #BlackLivesMatter has become a well-recognized social media hashtag associated with the movement. The hashtag is used to communicate to supporters about breaking news, real-time actions, or upcoming events.[47] The Black Lives Matter

42. *Id.*

43. PEN AMERICAN CENTER, GLOBAL CHILLING: THE IMPACT OF MASS SURVEILLANCE ON INTERNATIONAL WRITERS 1, 5 (2016), www.pen.org/sites/default/files/globalchilling_2015.pdf.

44. *Id.* at 13.

45. *Id.* at 10.

46. *See* Joseph, *supra* note 22.

47. Stephen, *supra* note 3.

movement is not one that resides under one monolithic institution but is a more diffused movement that is facilitated by the social media technologies of today.[48]

This heavy use of social media has also made it a target of social media monitoring.[49] The Department of Homeland Security began monitoring Black Lives Matter when the protests in Ferguson began and collected information "from public social media accounts, including on Facebook, Twitter, and Vine, even for events expected to be peaceful."[50] This is also not the first time DHS has engaged in social media monitoring. Documents previously obtained by the Electronic Privacy Information Center ("EPIC") showed that DHS previously contracted with General Dynamics to monitor, in general, the news, specifically social media, for any reports that reflected badly on DHS or the U.S. Government.[51]

Social media monitoring turns those exercising their First Amendment rights into targets of government surveillance, and such surveillance will have a chilling effect.[52] Unfortunately, the law is currently of little help to prevent this kind of widespread surveillance of social media. This legal vacuum is exacerbated by the fact that the government often outsources social media monitoring to the private sector. These companies are often very secretive about the methods they use for social media monitoring, the vastness of their collection, and the algorithms they use to analyze all the data they ingest from the monitoring of social media.[53] Such secrecy prevents the public from understanding the extent of the monitoring of social media, whether the algorithms produce bias results, or even if the social media monitoring is effective by any measure.

V. HOW THE CURRENT STATE OF THE LAW PROVIDES LITTLE PROTECTION

The law currently provides little recourse to protect publicly available social media posts and information from government monitoring. Although the mass gathering and analysis of social media data implicates the First and Fourth Amendments, current case law does not adequately support the use of either Amendment to curb the mass surveillance of social media.

Under the Fourth Amendment, we have a reasonable expectation of privacy.[54] The reasonable expectation of privacy test was first articulated in the concurrence

48. *Id.*

49. *See* Joseph, *supra* note 22.

50. *Id.*

51. *EPIC v. Department of Homeland Security: Media Monitoring,* ELECTRONIC PRIVACY INFO. CTR., https://epic.org/foia/epic-v-dhs-media-monitoring/ (last visited Feb. 15, 2017).

52. *See* Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMM. Q. 296, 296–97, 307 (2016).

53. *Id.* at 299.

54. *See generally* Katz v. United States, 389 U.S. 347 (1967).

by Justice Harlan in *Katz v. U.S.*[55] In *Katz*, the government had placed an electronic listening device outside a public phone booth to listen to the defendant's phone conversation.[56] The government used the defendant's side of the conversation as evidence in the case over the objection of the defendant.[57] Katz argued that the phone booth was a constitutionally protected space under the Fourth Amendment; the government argued that the phone booth was not constitutionally protected.[58]

The Court rejected the parties' formulation of the issue that focused on whether the phone booth was a constitutionally protected area, famously stating "the Fourth Amendment protects people, not places."[59] The Court explained that "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.[60] Based on this formulation of the issue, the Court found that "The Government's activities in electronically listening to and recording the petitioner's words *violated the privacy upon which he justifiably relied* while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[61] In other words, Katz had a reasonable expectation of privacy in his conversation in the phone booth. Having found that a search was conducted, the Court went on to analyze whether the search was justifiable under the Constitution and found no justification.[62] The Court consequently reversed petitioner's conviction since the search was the basis for it.[63]

The majority opinion alluded to the "reasonable expectation of privacy" test, but it was in Justice Harlan's concurrence that the specific test, as we know it, was expressed. In his concurrence, Justice Harlan articulated his understanding of the emerging rule used in *Katz* and prior decisions, stating "that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[64]

As articulated and applied, the reasonable expectation of privacy test does not generally extend to information that "a person knowingly exposes to the public."[65]

55. *Id.* at 361–62 (Harlan, J., concurring).
56. *Id.* at 348 (majority opinion).
57. *Id.*
58. *See id.* at 351.
59. *Id.*
60. *Katz*, 389 U.S. 347, 351 (1967)
61. *Id*. at 353 (emphasis added).
62. *Id.* at 354–59.
63. *Id.* at 359.
64. *Id.* at 361 (Harlan, J., concurring).
65. *Id.* at 351 (majority opinion).

Social media posts that lack any security access are freely exposed to the public.[66] So, although I may have a subjective expectation of privacy in the totality of my public social media posts and any information that can be derived from the analysis of my social media, this subjective expectation of privacy is not one the courts have recognized as accepted by the public.[67]

Privacy in digital public space is not only undermined by the current reasonable expectation of privacy test, but it is complicated by the Third Party Doctrine, which gives no privacy protection to information freely given to a third party. The origins of the Third Party Doctrine start with *U.S. v. Miller*.[68] In that case, the defendant, Miller, claimed Fourth Amendment protections for his banking records that were accessed by the government without a judicial warrant.[69] The Court ruled that Miller had no Fourth Amendment interest in his bank records that were revealed and consequently conveyed to the government by a third party (i.e. the bank).[70] The Third Party Doctrine was largely solidified in *Smith v. Maryland*.[71] In *Smith*, the Court ruled that the defendant did not have a Fourth Amendment interest in the phone numbers he dialed that were consequently passed to the phone company and then collected by the government, stating "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[72]

Because social media content is held by the companies that run the social media platforms, even social media users who restrict access to their social media content will not have Fourth Amendment protections over this information because it is held by a third party.[73] This fact allows government actors to obtain social media information directly from companies without a warrant. Although the Court in *U.S. v. Jones* began to recognize the problems with the Third Party Doctrine in a digital age,[74] the cases that estabished the doctrine still remain precedent.

In *U.S. v. Jones*, the government installed a Global Positioning System ("GPS") tracking device on a vehicle used by Jones.[75] The GPS device was installed on the

66. *See generally* S. Srinivansan, *Lack of Privacy Awareness in Social Networks*, 6 ISACA J., 2012, AT 1, 2–3 (explaining that social media privacy is often ignored unwittingly, and that users seem to overlook the possibility that personal information could be released to unintended people).

67. *See* Renee M. Jackson, *No Reasonable Expectation of Privacy in Content Posted to Social Networking Websites, Regardless of Individual Privacy Settings*, NIXON PEABODY LLP, Oct. 13, 2010, at 1, http://www.nixonpeabody.com/files/Employment_Law_Alert_10_13_2010.pdf.

68. *See generally* 425 U.S. 435 (1976).

69. *Id.* at 436.

70. *Id.* at 445.

71. *See generally* 442 U.S. 735 (1979).

72. *Id.* at 745.

73. *See generally* Jackson, *supra* note 67.

74. *See generally* 565 U.S. 400 (2012).

75. *Id*. at 403.

vehicle while it was on private property the day after the warrant expired and in Maryland instead of the District of Columbia, which is where the warrant authorized installation.[76] The government subsequently tracked the vehicle for 28 days.[77] The Court reviewed the lower court's decision that the warrantless attachment of the GPS device and subsequent tracking constituted a search and violated the Fourth Amendment.[78] In the majority opinion by the Court, written by Justice Scalia, the Court did not analyze whether a search occurred using the reasonable expectation of privacy test, instead it used the common-law trespassory test.[79] Justice Scalia wrote "When the Government physically invades personal property to gather information, a search occurs."[80] With respect to collecting the same GPS data without a trespass, Justice Scalia suggested "It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[81]

Despite the majority opinion in *Jones* not addressing whether the GPS tracking for an extended period of time constituted a search under the reasonable expectation of privacy test, majority support emerged in the concurrences. Both Justice Alito and Justice Sotomayor wrote concurrences supporting a reasonable expectation of privacy analysis that found that the GPS tracking constituted a search under the Fourth Amendment.[82] Justice Alito's concurrence was joined by Justices Ginsburg, Breyer, and Kagan.[83] Those four justices combined with Justice Sotomayor constitute what has been referred to as a "shadow" majority since the reasoning in the concurrences was not the basis of the majority opinion, but does suggest that the Court would have considered long-term GPS tracking a search under the reasonable expectation of privacy test.

Both the Alito concurrence and Sotomayor concurrence show concern for the prospect of conducting the same exact gathering of GPS data as in the present case but without any physical intrusion.[84] But, it is Justice Sotomayor who acknowledges the growing issue of the Third Party Doctrine in our digital society, stating:

> *[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to*

76. *Id.*
77. *Id.*
78. *Id*. at 404 (citing United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010)).
79. *Id.* at 409.
80. *Jones*, 565 U.S. at 414.
81. *Id*. at 412.
82. *Id*. at 413–18 (Sotomayor, J., concurring); *Id*. at 418–19 (Alito, J., concurring).
83. *Id*. at 418 (Alito, J., concurring).
84. *Id*. at 413–18 (Sotomayor, J., concurring); *Id*. at 418–19 (Alito, J., concurring).

> *third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.*[85]

This indication that the Court should reconsider the Third Party Doctrine is a step in the right direction, if only a very minor one. Unfortunately, social media information freely exposed to the public may need more than new precedent that overturns the Third Party Doctrine. In the cases that established the Third Party Doctrine, the data in question was only given to a distinct and definable third party, leaving room to distinguish social media data because of the fact it is freely exposed to the public. On the other hand, many of the risks associated with GPS tracking highlighted by Justice Sotomayor in her concurrence are applicable to social media monitoring. For example, in *Jones*, Justice Sotomayor acknowledges the chilling effect to First Amendment associational and expressive freedoms.[86] A similar chilling effect occurs with social media monitoring that analyzes everything you say and everyone you are connected to on social media.

The current trends exposed by social media monitoring, including sophisticated algorithms to analyze not only the social media connections but the publicly available content requires more robust protections if we are to provide adequate protections for our First Amendment rights. Merely protecting the associations will not be enough when the expressions are also the subject of large-scale collection and analysis.

VI. TO FILL THE VACUUM, COMMUNITY INVOLVEMENT AND NEW REGULATION ARE NEEDED

Given the expansiveness of the monitoring of social media, and the increasing surveillance and analysis of other publicly available data across the country, the installation of community oversight at the local level and baseline protection at the federal level are essential.

Regulations that allow for better community oversight of current and new surveillance technologies are necessary to appropriately protect our privacy and First Amendment rights. Furthermore, regulation is also needed at the federal level to provide baseline protections against unfettered government analysis of social media and other publicly available data (particularly digital data).

City councils across the country would be wise to look at the Surveillance and Community Safety Ordinance being considered in Oakland, California. The ordinance recently and unanimously passed out of Oakland's Privacy Advisory

85. *Id.* at 417 (Sotomayor, J., concurring).

86. 565 U.S. at 416.

Commission and is currently up for consideration by the Oakland City Council.[87] The Surveillance and Community Safety Ordinance represents a model law to address the increasing use of surveillance and provides a framework for combating the unnecessary introduction or overly expansive use of new mass surveillance technology like social media monitoring.[88] The Oakland ordinance arose out of "Oakland's effort to build the Domain Awareness Center, a city-wide surveillance hub that would have monitored people's activities from a variety of cameras and sensors."[89]

There are a number of important features in the ordinance to ensure that public mass surveillance technologies are included within its purview, that public input is considered, and that safeguards are put in place prior to deployment of new surveillance technology.

First, the Oakland ordinance recognizes that even the collection of purely publicly available data needs to be addressed. The ordinance allows for scrutiny of surveillance "technology which aggregates publicly available information" as such technologies "ha[ve] the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations."[90] Social media monitoring is clearly a "technology which aggregates publicly available information."[91]

Second, "meaningful public input" on "how surveillance technologies should be funded, acquired, or used" is required.[92] And, the expectation is that the public's opinion will be "given significant weight."[93] Such discussions beforehand allow the community impacted by mass surveillance technology to clearly define their expectation of privacy.

Third, "legally enforceable safeguards, including robust transparency, oversight, and accountability measures must be in place . . . before any surveillance technology is deployed."[94] Often where new surveillance technology is incorporated, there are not enough measures put in place to ensure appropriate usage of the technology.

87. Cyrus Farivar, *Oakland May Become Rare American City With Strict Rules for Spy Gear Use*, ARSTECHNICA (Jan. 6, 2017), https://arstechnica.com/tech-policy/2017/01/oakland-may-become-the-rare-american-city-with-strict-rules-for-spy-gear-use.

88. *See* Oakland, Cal., The Surveillance and Community Safety Ordinance (Jan. 5, 2016) (Draft), http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/report/oak062224.pdf.

89. Darwin BondGraham, *Oakland Privacy Commission Approves Surveillance Transparency and Oversight Law*, EAST BAY EXPRESS (Jan. 6, 2017), http://www.eastbayexpress.com/SevenDays/archives/2017/01/06/oakland-privacy-commission-approves-surveillance-transparency-and-oversight-law.

90. Oakland, Cal., The Surveillance and Community Safety Ordinance (Jan. 5, 2016) (Draft), http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/report/oak062224.pdf.

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.*

Incorporating transparency, oversight, and accountability measures upfront helps prevent new surveillance technology from expanding beyond its originally stated use. To assist with the transparency and oversight, the Oakland ordinance requires data reporting that allows the public and the city council "to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to."[95]

At the federal level, a straightforward regulation should be implemented that requires a warrant to perform data analysis of information collected through mass public surveillance.

New regulation would make clear that indiscriminate social media monitoring constitutes a search under the Fourth Amendment and a violation of First Amendment freedoms, thus providing individuals a means to challenge authorities who improperly monitor the social media account of an individual.

VII. CONCLUSION

Even considering the amount of data that is already gathered about us on a daily basis, we are still at the beginning of the datafication of our lives and analysis of that data. Social media monitoring is the current example of the perils to our democracy posed by the gathering and analyzing of data from public spaces. There will be more. If we are to maintain a viable democracy, it is paramount that we consider the consequences of mass surveillance and analysis—including and especially of our public space—which lacks protections to preserve any sense of privacy in public.

95. *Id.*