epic.org ELECTRONIC PRIVACY INFORMATION CENTER

Spotlight on Surveillance – June 2018

Social Media Monitoring: Government Surveillance of Public Space

I. Introduction

EPIC's Spotlight on Surveillance project explores the privacy and civil liberties implications of varying surveillance techniques and capabilities. This report, in particular, focuses on government social media monitoring.
Through a Freedom of Information Act request in 2011, EPIC was the first to uncover information about social media monitoring by a federal agency.[1] In EPIC v. DHS, EPIC obtained nearly 300 pages of documents about the Department of Homeland Security's monitoring of social media data.[2] The documents clearly showed that the monitoring program was more expansive than DHS had communicated to the public.

DHS paid General Dynamics to monitor "public social communications on the Internet." DHS stated that the purpose of the program was to identify threats to public safety and national security.[3] But the records EPIC obtained demonstrated that DHS was also monitoring the political views of Americans. [4] DHS secretly tracked public comments on policy debates related to the department activities.[5] Monitoring was triggered with ambiguous key terms, such as "subway," "drug," and "virus."[6] DHS monitored the Internet for criticisms of the DHS and maintained name identified records..[7]

As a result of EPIC's findings, the House Committee on Homeland Security undertook an investigation and convened a hearing on "DHS Monitoring of Social

[1] EPIC, *EPIC v. Department of Homeland Security: Media Monitoring* (2018), https://www.epic.org/foia/epic-v-dhs-media-monitoring/.
[2] Charlie Savage, *Federal Contractor Monitored Social Network Sites*, The New York Times (Jan. 13, 2012), https://www.nytimes.com/2012/01/14/us/federal-security-program-monitored-public-opinion.html.
[3] Id.
[4] EPIC, *EPIC v. Department of Homeland Security: Media Monitoring* (2018).
[5] Charlie Savage, *Homeland Analysts Told to Monitor Policy Debates in Social Media*, The New York Times (Feb. 22, 2012), https://www.nytimes.com/2012/02/23/us/house-questions-homeland-security-program-on-social-media.html.
[6] NBCNews, List reveals keywords feds monitor on Facebook, Twitter (Feb. 28, 2012), https://www.nbcnews.com/technology/list-reveals-keywords-feds-monitor-facebook-twitter-241271
[7] *See* Jaikumar Vijayan, *DHS Media Monitoring Could Chill Public Dissent, EPIC Warns*, Computer World (Jan. 16, 2012), https://www.computerworld.com/article/2501377/security0/dhs-media-monitoring-could-chill-public-dissent--epic-warns.html.

Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy."[8] At the hearing, members of both parties scrutinized DHS officials over the details of the agency's social media monitoring program revealed by EPIC's FOIA lawsuit.[9] Members of the subcommittee agreed with EPIC that the program had a chilling effect and expressed support for EPIC's proposal to suspend the program.[10]

EPIC's disclosure of the DHS social media monitoring program in 2012 and the resulting scrutiny arguably curbed the expansion of these type of programs at the time, but there is today renewed interest in government use of social media monitoring.[11] This report explores recent developments in government social media monitoring; provides examples of systems used to monitor social media; and discusses government regulation (and the lack thereof). The report concludes with a summary of major privacy and civil liberties risks arising out of increased use of social media monitoring and EPIC's recommendations.

II. Social Media Monitoring Technology

Social media monitoring software (SMMS) has significantly expanded over the past several years. Fortune 500 companies, politicians, law enforcement, federal agencies, defense contractors and even the military are purchasing SMMS products, such as XI Social Discovery, Geofeedia, Dataminr, Duanmi, MediaSonar, and SocioSpyder to name a few.[12] The CIA even has a venture fund, In-Q-Tel, that invests in SMMS technology.[13]

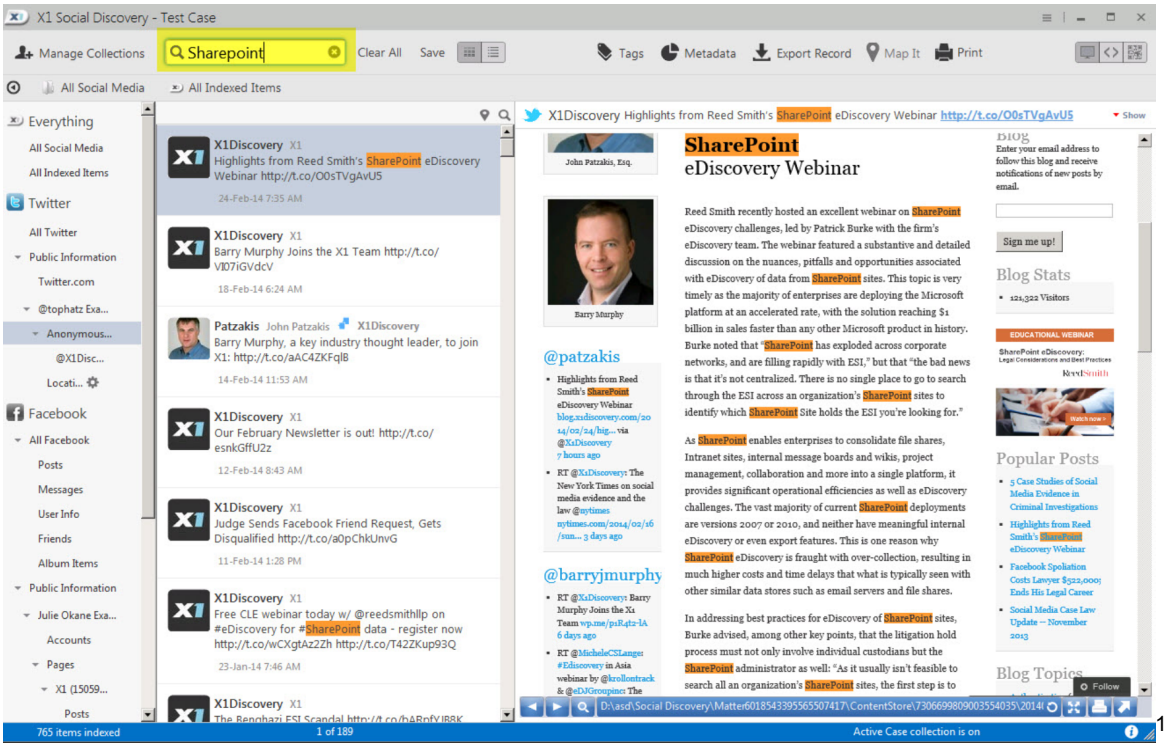
Social media monitoring technology enables law enforcement to constantly monitor and archive information on millions of people's activities. Law enforcement can probe posts on sites like Facebook, Twitter, Instagram, and YouTube for information on breaking news, protests, potential threats, and more.

X1 Social Discovery

---

[8] *DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy: Hearing Before the Subcomm. on Counterrorism and Intelligence of the H. Comm. on Homeland Security*, 112th Cong. (2012).
[9] *See* Andrea Stone, *DHS Monitoring of Social Media Under Scrutiny By Lawmakers*, Huffington Post (Feb. 16, 2012), https://www.huffingtonpost.com/2012/02/16/dhs-monitoring-of-social-media_n_1282494.html.
[10] David Kravets, *Lawmaker Demands DHS Cease Monitoring of Blogs, Social Meida*, Wired (Feb. 16, 2012), https://www.wired.com/2012/02/dhs-media-monitoring/.
[11] *Homeland Security to Compile Database of Journalists, Bloggers,* Bloomberg Law, Apr. 5, 2018, https://biglawbusiness.com/homeland-security-to-compile-database-of-journalists-bloggers/; *See also* EPIC v. DHS, No. 18-1268 (D.D.C. filed May 30, 2018) (seeking records and a Privacy Impact Assessment for a DHS system for "Media Monitoring Services").
[12] Kimberly McCullough, *Why Government Use of Social Media Monitoring Software is a Direct Threat to our Liberty and Privacy*, ACLU (May 6, 2016), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/why-government-use-social-media-monitoring.
[13] Lee Fank, *The CIA is Investing in Firms that Mine your Tweets and Instagram Photos*, The Intercept (April 14, 2016), https://theintercept.com/2016/04/14/in-undisclosed-cia-investments-social-media-mining-looms-large/.

X1 Social Discovery "aggregates comprehensive social media content and web-based data into a single user interface, collects vital metadata in a legally defensible manner and preserves the chain of custody."[14] Unlike other mechanisms that archive and image capture social media posts, X1 Social Discovery produces content through "searchable native format," which preserves metadata.[15]



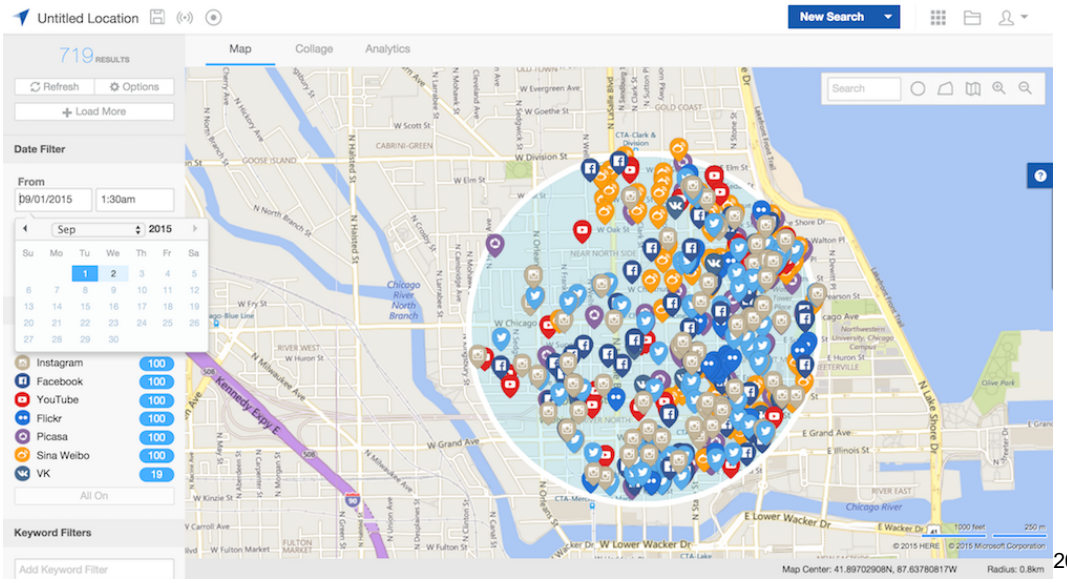
[16]

Geofeedia

Geofeedia is an intelligence platform that collects social media posts from Instagram, Twitter, Periscope, Vine, YouTube and Sina Weibo, and associates it with geographic locations.[17] The Los Angeles County Sheriff's Department was a major client, enabling the Department to visualize posts in an area in real-time and analyze the contents. The company's technologies have been reportedly used by law enforcement to identify and arrest protestors in events such as the 2015 Balitmore

[14] X1 Social Discovery, *Social Media and Internet-Based Data Collection*, https://www.x1.com/products/x1_social_discovery/.
[15] Id.
[16] Digital Forensics, *X1 Social Discovery Software Perpetual*, https://shop.avatu.co.uk/shop-by-category/Forensic-Imaging-Software/social-discovery-software-perpetual-license.
[17] Richard Byrne Reilly, *Geofeedia geolocates your social media postings, reaps $3.5M*, Venture Beat, https://venturebeat.com/2014/10/15/geofeedia-geolocates-your-social-media-postings-reaps-3-5m/.

protests that followed the death of Freddie Gray.[18] As a result, Facebook, Instagram, and Twitter restricted Geofeedia's access to user data.[19]



[20]

MediaSonar

MediaSonar is a company, headquartered in London, Ontario, that sells social media monitoring software. The software serves as an intelligence platform that aggregates and filters data. Like Geofeedia, the software was reportedly sold to California law enforcement agencies and used to track protesters using specific hashtags in their posts.[21]

Dataminr

Dataminr is an international real-time information discovery company.[22] Its technology can detect, qualify and classify public information in real time and "discover high impact events and critical breaking news far in advance of existing information systems."[23]

---

[18] Nicole Ozer, *Police Use of Social Media Surveillance Software is Escalating, and Activists are in the Digital Crosshairs*, ACLU (Sept. 22, 2016), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/police-use-social-media-surveillance-software.

[19] Lora Kolodny, *Facebook, Twitter cut off data access for Geofeedia, a social media surveillance startup*, TechCrunch (Oct. 11, 2016), https://techcrunch.com/2016/10/11/facebook-twitter-cut-off-data-access-for-geofeedia-a-social-media-surveillance-startup/.

[20] Anthony Ha, *Geofeedia Raises $17M to Help Businesses Tap Into Social Location Data*, Tech Crunch (Feb. 3, 2016), https://techcrunch.com/2016/02/03/geofeedia-series-b/.

[21] Jordan Pearson, *Facebook banned this Canadian surveillance company from accessing its data*, Motherboard (Jan 19, 2017), https://motherboard.vice.com/en_us/article/yp3jw5/instagram-banned-this-canadian-surveillance-company-from-accessing-its-data-media-sonar.

[22] Dataminr, *About*, https://www.dataminr.com/about?gclid=EAIaIQobChMIufKd37SU2AIVTLnACh3FYwB8EAAYASABEgLcVvD_BwE.

[23] Crunchbase, *Dataminr*, https://www.crunchbase.com/organization/dataminr.

[24]

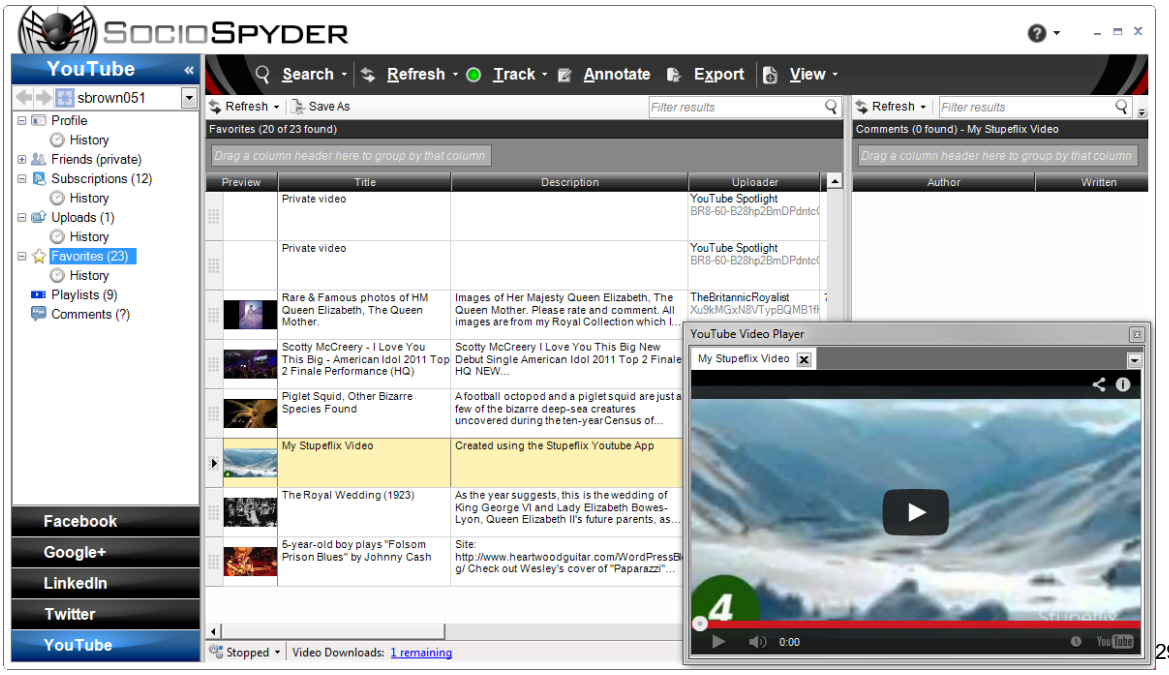
SocioSpyder

SocioSpyder is an investigative software that "gathers open source information from many popular social media platforms, while minimizing the footprint left by investigative teams."[25] The software enables analysts to "download and retain social media content on-demand or autonomously" and "apply annotations and visualizations to stored data, then share with investigative teams."[26] It can be "configured to collects posts, tweets, videos and chats on-demand or autonomously into a relational, searchable and graphable database." This function enables analysts to keep tabs on both the different targets across various social networks simultaneously, as well as download all of the data and store it.[27] It can also map out user-to-user relationships and graph the data it collects. According to the SocioSpyder website:

> With over 900 million Facebook users and 400 million daily tweets, finding incriminating data is sometimes overwhelming. But, mining and organizing data collected from these massive sources is paramount to the success of the 21st

[24] Josh Ong, *Dataminr launches a media-focused service that scans Twitter for breaking news*, The Next Web (Sept. 23, 2014), https://thenextweb.com/twitter/2014/09/23/dataminr-launches-media-focused-service-scans-twitter-breaking-news/.
[25] SocioSpyder, *Investigative Software*, https://www.sociospyder.com/.
[26] Id.
[27] Id.

century investigative agency. SocioSpyder is the key to solving the complexities of this multifaceted problem.[28]



[29]

In-Q-Tel

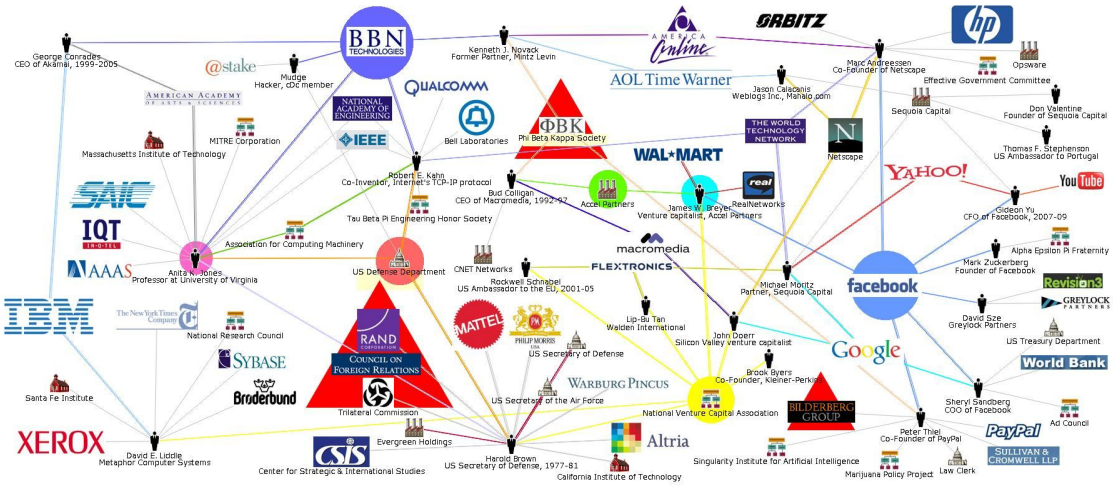
In-Q-Tel is a "strategic investor that accelerates the development and delivery of cutting-edge technologies to U.S. government agencies that keep our nation safe."[30] The company works to bridge "the gap between the challenging technology needs of the national security agencies, the rapidly changing innovations of the startup world, and the venture community that funds those startups."[31] In other words, the firm invests in high-tech companies solely to inform the Central Intelligence Agency (CIA) and other intelligence agencies of the latest information technology to support U.S. intelligence capabilities.[32] Among the software companies that In-Q-Tel invests in are Palantir and Visible Technologies, both offering services in social media monitoring.[33]

A series of reports have revealed the extent of the relationship between In-Q-Tel and U.S. intelligence agencies. For instance, in 2006, it was reported that the NSA installed data mining equipment called Narus STA 6400 that enabled the NSA to scoop up troves of Internet data from AT&T customer's internet traffic. In-Q-Tel invested in and

---

[28] Id.; *see also* Joseph Cox. *SocioSpyder: the Tool Bought by the FBI to Monitor Social Media*, Motherboard (Feb. 23, 2016), https://motherboard.vice.com/en_us/article/8q8g73/sociospyder-the-tool-bought-by-the-fbi-to-monitor-social-media.
[29] Id.
[30] In-Q-Tel, *About*, https://www.iqt.org/about-iqt/.
[31] Id.
[32] D&B Hoovers, *In-Q-Tel, Inc Company Information*, http://www.hoovers.com/company-information/cs/company-profile.In-Q-Tel_Inc.23e1db89928dd9e6.html.
[33] In-Q-Tel, *Our Portfolio*, https://www.iqt.org/portfolio/.

helped fund the company that created the Narus STA 6400.[34] Also, in 2009, another report revealed that In-Q-Tel invested in Visible Technologies, a company specializing in social media monitoring software.[35] The software monitors what people say on social media websites, including Twitter, Facebook, YouTube, Flickr and Amazon. The company's software is capable of real-time communications tracking, trend monitoring, and even sentiment analysis that categorizes blog posts and comments as positive or negative.[36] The Federal Reserve even issued a Request for Proposal for this type of social media monitoring software so that it could monitor communications surrounding its business.[37]



[38]

III. Government Use of Social Media Monitoring

a. Department of Homeland Security (DHS)

In February of 2017, DHS Secretary John Kelly testified at a House hearing on border security. In the hearing, Secretary Kelly discussed requiring visa applicants, refugees, or other foreign visitors to provide passwords for online accounts, including social media, in order to enter the United States. The Secretary also described plans to expand the use of "aerostats" (surveillance blimps) and monitoring of social media. Federal agencies gather social media comments to identify individuals critical of the government.

---

[34] Wired Staff, *AT&T Whistle-Blower's Evidence*, Wired (May 17, 2006), https://www.wired.com/2006/05/att-whistle-blowers-evidence/.

[35] Crunchbase, *Visible Technologies*, https://www.crunchbase.com/organization/visibletechnologies; Toby Harnden, *US spies invest in Internet monitoring technology*, The Telegraph (Oct. 20, 2009), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/6389669/US-spies-invest-in-internet-monitoring-technology.html.

[36] Id.

[37] Public Intelligence, *Federal Reserve Bank of New York Sentiment Analysis and Social Media Monitoring Proposal* (Sept. 26, 2011), https://publicintelligence.net/federal-reserve-bank-of-new-york-sentiment-analysis-and-social-media-monitoring-proposal/.

[38] GE TV, *Exposing 'In-Q-Tel,' CIA's Venture Capital Firm Investing in Technologies to Spy on You*, Global Elite TV (Apr. 8, 2016), https://globalelite.tv/2016/04/08/exposing-in-q-tel-cias-venture-capital-firm-investing-in-technologies-to-spy-on-you/.

On October 18, 2017, DHS posted updated language in the Federal Register about collecting "social media handles, aliases, associated identifiable information, and search results" on immigrants, including naturalized citizens and permanent residents. DHS's Customs and Border Protection (CBP) also published a system of records notice for the "Intelligence Records System." The system contains information including "raw intelligence information collected by CBP's [Office of Intelligence], public source information, and information initially collected by CBP pursuant to its immigration and customs authorities."[39] Public source data include social media, news media outlets, and the Internet.[40]

CBP uses two information technology systems to analyze data and develop finished intelligence products – the Analytical Framework for Intelligence (AFI) and the Intelligence Reporting System (IRS). These systems constitute the exclusive CBP System of Records Notice. AFI, in particular, enables CBP to search a broad range of data through a single interface, as well as identify links between individuals or entities based on commonalities – identification numbers, addresses, or other information.[41] AFI draws from a variety of federal, state, and local law enforcement databases that gather sensitive data about a person, including biographical information, personal associations, travel itineraries, immigration records, and home and work addresses, as well as fingerprints, scars, tattoos, and other physical traits. Palantir, a data-mining firm co-founded by Trump transition adviser Peter Thiel, has also assisted CBP and the Immigration and Customer Enforcement (ICE) operating the AFI.[42] CBP will use these systems to secretly profile and evaluate social media users.

CBP also proposed to exempt the database from many Privacy Act safeguards. The database contains detailed personal data from social media and commercial data services. CBP also proposed to create numerous "routine uses" for the information.[43]

ICE's original Extreme Vetting Initiative incorporated plans to monitor the Internet, including social media, to detect and flag individuals for deportation or visa denial. The Initiative was part of President Trump's January 2017 executive order, which contained a provision calling for the screening of every traveler to the U.S. The screening would be necessary to determine the likelihood that an individual would become "a positively contributing member of society" and "make contributions to the national interest," as well as "a mechanism to assess whether or not the applicant has

[39] Privacy Act of 1974: DHS/CBP – 024 Intelligence Records System (CIRS) System of Records, Notice (Sept. 21, 2017) [Hereinafter "CIRS Record Notice"] In, https://www.regulations.gov/document?D=DHS-2017-0027-0001.
[40] Id.
[41] CIRS Record Notice, *supra*.
[42] Spencer Woodman, *Documents suggest Palantir could help power Turmp's 'extreme vetting' of immigrants*, The Verge (Dec. 21, 2016), https://www.theverge.com/2016/12/21/14012534/palantir-peter-thiel-trump-immigrant-extreme-vetting
[43] Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-024 CBP Intelligence Records System (CIRS) System of Records, Proposed Rule (Sept. 21, 2017), https://www.regulations.gov/document?D=DHS-2017-0026-0001.

the intent to commit criminal or terrorist acts after entering the United States."[44] ICE recently dropped the agency's plan to incorporate extreme vetting software that would supposedly identify positively contributing verses potential terrorists.[45]

b. State Department

In June, 2017, the State Department formally implemented a questionnaire for a subset of visa applications that required the disclosure of their social media handles from the last five years.[46] The questions include email addresses, phone numbers, past addresses, previous employment and travel history. The Department emphasizes that the questions are voluntary; but, the questionnaire notes that failing to answer could delay or even prevent the visa's processing. In March 2018, the State Department expanded the questionnaire to all visa applicants.[47]

The State Department also uses social media monitoring as a "public relations strategy" that can "mitigate the worst impacts" of damaging events.[48] The strategy is to promote resiliency in responding to world events that threaten the national interest of the U.S. and its citizens. To do so, the Department uses real-time monitoring and identification and cultivation of key online influencers. The Rapid Response Unit within the Bureau of Public Affairs monitors social media responses to any events that may have a potential impact on U.S. national interests. They subsequently produce reports tracking online public responses to certain events or issues.[49] From this information, the Unit creates maps of "online influencers" to understand the roles of individuals and their degree of influence online. The Office of Audience Research then work to better understand the impact the State Department has online and how to improve its presence.[50]

---

[44] Executive Order, *Executive Order Protecting the Nation from Foreign Terrorist Entry into the United States* (Jan. 27, 2017), https://www.whitehouse.gov/presidential-actions/executive-order-protecting-nation-foreign-terrorist-entry-united-states/.
[45] Drew Harwell and Nick Miroff, *ICE Just Abandoned Its Dream of "Extreme Vetting" Software that Could Predict Whether a Foreign Visitor Would Become a Terrorist*, Washington Post (May 17, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist/.
[46] State Department, Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants (May 4, 2017), https://www.federalregister.gov/documents/2017/05/04/2017-08975/notice-of-information-collection-under-omb-emergency-review-supplemental-questions-for-visa.
[47] State Department, 60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa (Mar. 30, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-03-30/pdf/2018-06490.pdf.
[48] Fergus Hanson, Baked In and Wired: eDiplomacy@State, Foreign Policy at Brookings *19 (June 2016), https://www.brookings.edu/wp-content/uploads/2016/06/baked-in-hansonf-5.pdf.
[49] Id. at 20.
[50] Id.

c. Federal Bureau of Investigation (FBI)

According to FBI contracting documents, the FBI has hired Dataminr to monitor in real-time more than 500 million daily tweets.[51] Dataminr uses public social media platforms to detect early "indications of high-impact events and critical breaking information" and transforms them into real-time alerts for its clients.[52] The FBI also bought SocioSpyder, another tool to monitor social media.[53] Public records show that the FBI purchased SocioSpyder and services related to its maintenance from August 2014 up to September 2015.[54] The U.S. Marshals was also noted to have purchased SocioSpyder.

d. State Governments

The Oregon Department of Justice reportedly used a tool called the Digital Stakeout, a social media monitoring software used to surveil people.[55] The software can be used to covertly monitor, collect, and analyze social media data from various platforms, including Twitter, Facebook, and Instagram.

Attempts to map the use of social media monitoring by law enforcement show that over 157 jurisdictions have spent at least $10,000 on social media monitoring software and only 18 of those have public policies regarding the use of social media monitoring.[56]

---

[51] FedBizOpps.gov, *Social Media Awareness – Indicators & Warnings* https://www.fbo.gov/index?s=opportunity&mode=form&id=4a9f7905fae17d11b64f69832474265d&tab=core&tabmode=list&=.

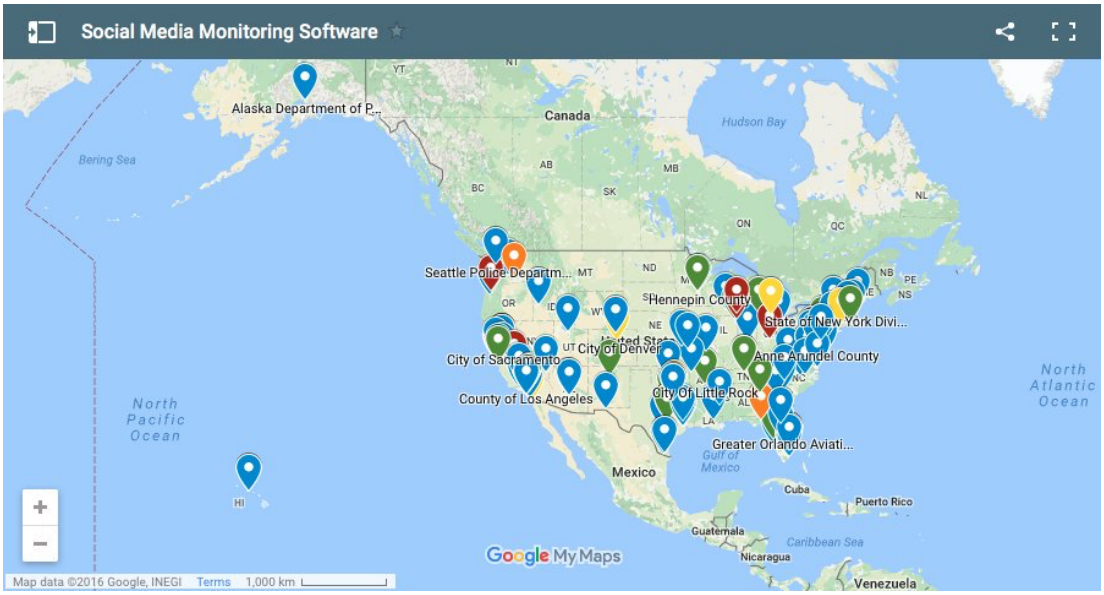
[52] Dataminr, *About*, https://www.fbo.gov/index?s=opportunity&mode=form&id=4a9f7905fae17d11b64f69832474265d&tab=core&tabmode=list&=.

[53] Joseph Cox, *SocioSpyder: the Tool Bought by the FBI to Monitor Social Media*, MotherBoard (Feb. 23, 2016), https://motherboard.vice.com/en_us/article/8q8g73/sociospyder-the-tool-bought-by-the-fbi-to-monitor-social-media.

[54] Public records can be found at: https://www.fpds.gov/ezsearch/fpdsportal?q=allied+associates+CONTRACTING_AGENCY_NAME:%22FEDERAL+BUREAU+OF+INVESTIGATION%22&s=FPDS&templateName=1.4&indexName=awardfull&x=0&y=0.

[55] ACLU of Oregon, *#BlackLivesMatter Tracked by Oregon DOJ with Social Media Monitoring Software*, ACLU (May 4, 2006), https://www.aclu-or.org/en/news/blacklivesmatter-tracked-oregon-doj-social-media-monitoring-software.

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



Other reports revealed that the local police department in Fresno was using MediaSonar, a social media surveillance tool, to identify "threats to public safety" by monitoring hashtags, including #BlackLivesMatter, #DontShoot, #ImUnarmed, #PoliceBrutliaty, and #ItsTimeforChange.[57] Subsequently, the public records were requested from 63 police departments, sheriffs, and district attorneys across California.[58] The records revealed that 40% of the agencies (20 total) utilize social media monitoring tools and have done so without any public notice, debate, community input, or lawmaker vote.[59] These agencies have been using MediaSonar, X1 Social Discovery, and Geofeedia, along with other surveillance tools to monitor online behavior.[60] Geofeedia, in particular, was noted to flag activist groups as "over threats" and at least 13 California law enforcement agencies have made use of the program.

[57] Ozer, *supra*.
[58] Id.
[59] Id.
[60] Id.

[61]

IV. EPIC's Work

EPIC is a leader in the fight to protect privacy interests and develop greater transparency of social media monitoring practices. In a FOIA lawsuit EPIC v. CBP, EPIC uncovered Palantir's role in Analytical Framework for Intelligence, a program that uses vast amounts of information—including social media data, to assign "risk assessment" scores to U.S. travelers. EPIC has also pursued a FOIA request to Immigration and Customs Enforcement seeking details of the agency's relationship with Palantir. In 2017, EPIC sent a letter to the Senate Finance Committee regarding CBP's collection of social media information. EPIC also submitted comments to the Department of Homeland Security and CBP concerning the collection of social media information.

In the comments to CBP, EPIC opposed the federal agency's proposal to collect social media information, including metadata, for a new intelligence database. CBP also proposed to exempt the database from protections of the Privacy Act and to create numerous "routine uses" for the information. EPIC said that CBP should narrow the Privacy Act exemptions and limit the number of routine uses.

EPIC joined the Fly Don't Spy! campaign to urge DHS Secretary Kelly to reject plans to require to hand over passwords to the federal government. Such a requirement would undermine privacy and human rights, chill freedom of speech and association, and create greater security risks for travelers. Earlier this year, Secretary Kelly testified before Congress about collecting social media passwords. The Secretary described plans to expand the use of "aerostats" (surveillance blimps) and monitoring of social

[61] Id.

media. In response, EPIC immediately filed a FOIA request regarding all DHS plans to user individuals' Internet and social media information to vet potential entrants to the U.S.

In a FOIA lawsuit against DHS, EPIC obtained documents that revealed federal agencies gather social media comments to identify individuals critical of the government. EPIC is also pursuing a FOIA request about a revised DHS plan to require disclosure of social media passwords before allowing entry into the country.

In comments to DHS, EPIC opposed a plan to add social media information to the official files of all immigrants. EPIC said the DHS proposal threatens First Amendment rights, risked abuse, and would disproportionately impact minority groups. A coalition of organizations also submitted comments to express concern about the proposal.

EPIC and a coalition of civil rights organizations have also urged the Acting Secretary of Homeland Security to end the Extreme Vetting Initiative. The 'Extreme Vetting' Initiative uses opaque procedures, secret profiles, and obscure data including social media posts, to review visa applicants and make final determinations.

In comments to the State Department, EPIC urged the agency to drop a plan to obtain the social media identifiers of a subset of individuals applying for visas to enter the U.S. EPIC argued that the proposal threatens important First Amendment rights, risked, abuse, and would disproportionately impact certain minority groups. When the State Department decided to collect social media identifiers from all visa applicants, EPIC and a coalition of over 55 privacy, civil liberties, and civil rights groups urged the State Department to withdraw the proposal.[62]

EPIC has previously opposed DHS proposals to collect social media information and recently submitted a FOIA request following statements made by the Homeland Security Secretary, indicating DHS planned to ask individuals for social media passwords before allowing entry in the U.S. According to FBI contracting documents, the FBI has hired Dataminr to monitor in real-time more than 500 million daily tweets. EPIC has warned that these techniques of mass surveillance will subject more innocent people to government investigation.

V. Privacy and Civil Liberties Concerns:

Privacy and civil liberties groups have expressed many risks with government use of social media monitoring:

- It will chill free speech. Immigrants and foreign visitors will begin to censor themselves online in response to growing and continuous scanning of social media platforms (Facebook, Twitter, Instagram, LinkedIn, etc.). As EPIC's prior

[62] Comments of the Brennan Center, EPIC, *et. al*, *60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa* (May 29, 2018), https://epic.org/privacy/Coalition-Comments-DOS-Visa-Social-Media-Collection-May2018.pdf.

FOIA lawsuit against DHS revealed, federal agencies are using social media monitoring to monitor political opinions.[63] Even Congress recognized the impact this would have on free speech and has held oversight hearings.[64]

- It discriminates. Courts have found that the criteria used to vet and flag individuals are arbitrary and designed to target minorities, such as Muslims.[65] ICE has broad discretion to deport or exclude anyone by utilizing such criteria, which includes looking to whether an individual will contribute to "society" or the "national interest."[66] As the 2012 EPIC lawsuit revealed, federal agencies also use biased and ambiguous search terms that discriminate.[67] For example, DHS pinpoints individual countries, such as "Iraq," "Afghanistan," "Iran," and "Pakistan."[68] DHS also flagged key terms such as "prevention," "initiative," "power," and even "social media." The expansive nature of the search contributes toward discriminatory monitoring as federal agencies obtain a massive trove of data to sift through as they please.

- Social media monitoring is unreliable and ripe with problems. Take, for example, the Extreme Vetting Initiative. The government is proposing to deport or exclude individuals by determining whether their online behavior will contribute to society or are likely to engage in acts of terrorism. Making decisions based on social media information is complex. The current systems can't automatically compute risks of terrorist behavior and computers will not likely solve the problem.[69] One mistake can result in "wrongful denials of entry, arrests and worse, while retaining sensitive information on people's social media habits may endanger immigrants in their home countries and threaten the free expression of non-U.S. citizens and citizens alike."[70]

- Social media monitoring can cause irreversible harm. Take, for example, the following real-life scenario: a Palestinian construction worker posted a photo of himself leaning against a bulldozer near the West Bank with a cup of coffee and a lit cigarette. The caption for the photo was in Arabic and translated to "good

---

[63] Savage, *supra*.
[64] Id.
[65] *See* State of Hawaii v. Trump, No. 17-15589 (June 12, 2017), http://www.cnn.com/2017/06/12/politics/9th-circuit-ruling-travel-ban/index.html; Laura Jarrett and Ariane de Vogue, *9th Circuit deals Trump travel ban another defeat*, CNN (June 13, 2017), http://www.cnn.com/2017/06/12/politics/9th-circuit-travel-ban/index.html.
[66] Brennan Center for Justice, *ICE Extreme Vetting Initiative: A Resource Page* (Nov. 16, 2017), https://www.brennancenter.org/analysis/ice-extreme-vetting-initiative-resource-page.
[67] Reuven Cohen, *Dept. of Homeland Security Forced to Release List of Keywords Used to Monitor Social Networking Sites*, Forbes (May 26, 2012), https://www.forbes.com/sites/reuvencohen/2012/05/26/department-of-homeland-security-forced-to-release-list-of-keywords-used-to-monitor-social-networking-sites/2/#3f74ba407d90.
[68] Id.
[69] Id.
[70] Marissa Lang, *Social Media Monitoring Continues to Concern Civil Rights Groups*, Government Technology (Oct. 26, 2017), http://www.govtech.com/public-safety/Social-Media-Monitoring-Continues-to-Concern-Civil-Rights-Groups.html.

morning." A Facebook algorithm, however, translated one language to another and interpreted the caption as saying "attack them" in Hebrew and "hurt them" in English. The man was subsequently arrested and detained for several hours.[71]

VI. Recommendations

Federal, state, and local agencies that use social media monitoring should publish detailed policies and procedures, subject to public comments, that cover the collection, use, dissemination, and retention of data from social media. All name identified record systems must comply with the Federal Privacy Act, including both a Systems of Records Notice and a formal rulemaking process. The Privacy Act also prohibits the creation of record systems for individuals exercising First Amendment rights except in certain, narrow circumstances.[72] Any media monitoring, lacking authority established pursuant to public law, should end immediately.

For example, the State Department should withdraw the agency's proposal to collect the social media IDs of visa applicants; CBP should eliminate the collection of social media in the agency's CIRS intelligence database; and the FBI should cease the mass, indiscriminate surveillance of tweets.

Legislation on social media monitoring should prohibit the mass social media monitoring of innocent individuals and require a warrant or a narrowly tailored emergency exception for its use. Additionally, legislation should implement transparency requirements regarding the use of social media monitoring and mechanisms for oversight, including independent audits of its use.

Social media is a public space where ideas are exchanged, debates are had, and new connections are made. It should not be a space of constant monitoring by the government that threatens our First Amendment rights and undermines our democracy.

---

[71] Yotam Berger, *Israel Arrests Palestinian Because Facebook Translated 'Good Morning' to 'Attack Them*,*'* Haaretz (Oct. 22, 2017), https://www.haaretz.com/israel-news/1.818437.

[72] 5 U.S.C. § 552a(e)(7) ("Agency requirements") states:

> —Each agency that maintains a system of records shall— . . .
> maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;