TechTank

BROOKINGS

Digital fingerprints are identifying Capitol rioters

Darrell M. West Tuesday, January 19, 2021

Recent years have seen a dramatic flourishing of digital technologies. In our book, "Turning Point: Policymaking in the Era of Artificial Intelligence," Brookings President John Allen and I describe major advances in social media, mobile technology, facial recognition, financial technology, and internet-based platforms over the past few decades. People are communicating via social media sites and text messages, exchanging money and finding lodgings online, and posting pictures and videos that document when, where, and at what time they engaged in various activities.

Following the mob violence at the U.S. Capitol on Jan. 6, 2021, it, therefore, is not surprising that many of these tools have been deployed to identify rioters, find those who engaged in violence and vandalism, and use that evidence to indict suspects. Many of the rioters left detailed digital fingerprints that document their movements, communications, viewpoints, and financing. Taken together, the information gathered before, during, and after the riot demonstrates how technology enables both insurrection and legal accountability.

Social media posts

Identifying rioters has been easy because many of them posted pictures of themselves inside the Capitol Building. They posed with Capitol Police, took selfies in Statutory Hall, on the floor of the Senate, and in the speaker's office, videotaped themselves and others rampaging through the building, and bragged publicly about their participation in the onslaught.

Through these actions, these individuals provided concrete evidence of illegal entry into the building, vandalism, assault, and mayhem. Unwittingly, they gave virtual confessions that would make Perry Mason or CSI attorneys squeal with delight. The public nature of this information has allowed law enforcement, investigators, and independent observers to piece together illegal behavior and identify possible perpetrators.

Social media also offers relevant material regarding planning and coordination on the part of rioters and legislators. There have been reports of a Republican House member using codewords for insurrection such as "Today is 1776" on the morning of the riots as a way to express support for participants. Others publicly posted information regarding the movements of Speaker Nancy Pelosi, one of the key targets of the rioters. While we do not yet know the full extent of the planning and coordination, there is enough evidence to warrant a serious look at legislator culpability.

Emails and text messages

Electronic communications represent another type of digital evidence. Individuals have been indicted for saying that they wanted to harm Pelosi, Vice President Mike Pence, and Washington, D.C. Mayor Muriel Bowser. One man sent a text warning he was "Ready to remove several craniums from shoulders." Another texted a friend admitting he was "one of the 700 inside." Without seeming to be aware of the likelihood that law enforcement would gain access to the messaging, he told someone he was "wanted by the FBI for illegal entry."

Photo identification

A number of individuals have been identified through facial recognition software and crowd-sourcing of video images. Facial recognition allows investigators in a criminal inquiry to attach names to specific pictures. According to Hoan Ton-That of facial recognition firm Clearview, "We have over 3 billion photos that we indexed from the public internet." That library as well as other image sources available to law enforcement allowed the FBI quickly to identify a number of perpetrators and charge them with

violence and vandalism. One suspect was surprised law enforcement was able to identify him so quickly after posting an Instagram photo of Pelosi's office complaining the picture "was up for only an hour."

Timeline and location

Digital communications are time-stamped such that very accurate timelines can be established. For example, social media posts, emails, text messages, and pictures have times down to the minute if not seconds. That information can enable prosecutors to establish very clear timelines for particular action. Putting all these digital markers together makes it possible to chart someone's activities over the course of a day. Having such detailed documentation is helpful to creating a legal narrative and establishing cause and effect between certain actions. Jurors who see a clear pattern of behavior leading to violence at a particular time generally find it easy to render a verdict.

Smartphones have GPS hardware and software that provide precise geolocation information. Between the phone itself and cell tower communications, law enforcement can determine where people were at specific times and use that as a basis for questioning suspects. It is hard to defend oneself when there is so much locational and timeline evidence in the possession of investigators.

Follow the money

In criminal investigations, it always is important to follow the money and find who financed travel, food, and lodgings for various suspects. Such information is relevant in terms of legal culpability as well as possible cases regarding planning, coordination, and conspiracy to commit sedition. It is easy to track bank transfers, mobile money transfers, and financial transactions. Unless one is using cash, there are digital fingerprints that document these actions in precise detail and that material can aid investigators seeking evidence on guilt or innocence.

Hotel and Airbnb accommodations

Airbnb offers inexpensive rentals for those wishing to visit Washington, D.C. For those wanting to avoid the cost and visibility of hotel accommodations, the platform offers a way to "fly below the radar" and stay away from large chains. Many people like the convenience of such accommodations. But because reservations are booked online, there is a record of who stayed where on particular days. When there are law enforcement investigations, AirBnB rental, as well as hotel accommodation records, can be accessed and turned over to authorities. Police officers can discover where people stayed and how they paid for the accommodations.

Dating sites

In early January, some D.C. residents noticed local dating sites showing profiles of newcomers who said they planned to be in town for a few days and wanted to meet local people. Some made veiled references to what turned out to be protest activities, while others wore clothing or displayed other evidence of sympathy to President Donald Trump.

Following the riots, enterprising women launched an effort to use dating sites as a way to identify those who may have participated in illegal activities. They went through profiles searching for possible suspects and sometimes held video chats in order to elicit riot-related confessions. In one online story, a woman said she advised her friends to "get on the apps and start screenshotting" for law enforcement. A number did and passed along the intelligence to law enforcement.

A learning opportunity

The culmination of all this online information is that it has been relatively easy to identify hundreds of rioters and indict many of them for criminal activities. Charges range from trespassing and disorderly conduct to vandalism and assault. Gathering detailed evidence is important not just for upcoming trials, but also for the historical record. What happened this month will be debated for decades to come, and we need clear evidence to document who was involved and what they did.

Yet at another level, it is crucial for all to be aware of how much online information exists and how easy it is to connect the dots. Once the investigation about the Capitol insurrection is completed and perpetrators brought to justice, there needs to be a national

conversation about the wealth of material that exists about everyone, including law-abiding citizens, and how that information is being used. The easy identification of insurrectionists should put everyone on guard about how much online personal data is available about all Americans. The breadth of data should concern even peaceful individuals and accelerate discussions regarding the need for national privacy legislation.