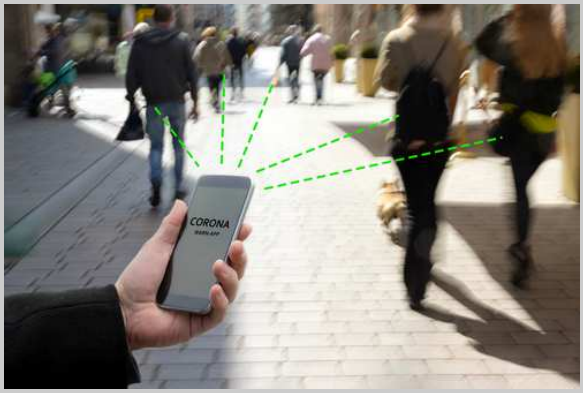
# SUMMER 2020 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, cybersecurity and data analytics needs. For this E-Newsletter, we provide an overview of workplace changes due to the Coronavirus, the implications of contact tracing technology, and litigation trends caused by COVID-19.

## Contact-Tracing Apps Raising Technical & Privacy Questions




Technology, like markets and governments, people and animals, changes in response to stress on the system. Historically, with war we have made leaps in medicine; population growth fostered advancements in farming; and the quest for space travel has required that we create out of this world technology. With near-continuous technological evolution, we've been able to mitigate some of the most potentially destructive events humans have faced for millennia, proving, if nothing else, that technology not only advances for the sake of advancement, but technology also responds. That technology is currently responding to the COVID-19 crisis shouldn't be a surprise. What may be a surprise though is that the technology being developed to address COVID-19 is raising questions of safety and privacy – two elements we expect our technology to address.

**Contact Tracing: Automating the Human Touch**

Contact tracing is the time-tested process of identifying persons who have been near a person who has received a confirmed diagnosis of a contagious illness. The key factor with regard to the efficacy of contact tracing is time: the faster potentially infected individuals can be identified, the faster they and the medical community can respond, and the faster the rate of infection can be quelled. So, of course, contact tracing seems like a natural fit for a technological response. The near ubiquity of cellular phones and the speed and ease with which apps can be created has allowed for the creation of not one, but dozens of contact tracing apps already being installed on smart devices around the globe. If the process of alerting potential patients to their exposure is automated, notifications can take place in the nanoseconds it takes for data to travel across a cellular network, rather than the days required for human tracers to gather information, locate individuals, and make the contacts. Win-win, right? Apparently, not so fast.

**As Close as Your Phone**

Two tech giants, Apple and Google, have developed, as a cooperative effort, root technology to automate contact tracing. The application program interface, called Exposure Notifications, makes use of Bluetooth Low Energy ("BLE") technology, the same technology that works with a variety of peripheral devices such as fitness trackers and wireless headphones. Apps that use the Exposure Notifications API work by scanning for other BLE-enabled devices within a certain proximity. When another device is found, a timer begins counting, and at the five-minute mark, rolling proximity identifiers are exchanged between the two devices and stored on the devices. If a person receives a diagnosis, they are given a code to enter into the contact tracing app and the app goes to work messaging the devices which contain all the other rolling proximity identifiers from previous contact. Apple and Google maintain that no personally identifying information is collected by the API, but that isn't stopping concerns from being raised (https://blog.google/documents/58/Contact_Tracing_Bluetooth_Specification_v1.1_RYGZbKW.pdf).

**Trust Issues**

Despite assurances by Apple and Google that no personally identifying information is collected by the Exposure Notifications API, privacy watchers like the Electronic Frontier Foundation, The Brookings Institute, and the American Civil Liberties Union have all expressed concerns that contact tracing apps need to be judiciously developed and cautiously deployed to ensure that privacy rights are not violated and that data collection is limited to essential information held securely and for the shortest duration possible (https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/). While not created by Apple and Google, Care19, a contact tracing app rolled out by the states of North and South Dakota, was found to send location data to Foursquare, a data collection company that sells location data to marketers (https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/), highlighting just one of the reasons the public may be skeptical about adopting automated contact tracing.

**Numbers are Vital**

In order for automated contact tracing to have a positive impact on curbing the COVID-19 virus, the enrollment rate needs to be around 60% of the general population in the desired geographic area (https://www.brookings.edu/techstream/contact-tracing-apps-face-serious-adoption-obstacles/). In the case of the population of the United States, that 60% equates to roughly 197 million people. 197 million people would have to agree to install and use a contact tracing app on a compatible device. To date, one of the most successful global efforts in the use of automated contact tracing among democracies is Iceland, which has managed to enroll nearly 40% of its population (https://www.technologyreview.com/2020/05/11/1001541/iceland-rakning-c19-covid-contact-tracing/). The idea that the United States, where individual states are making the decisions as to which, if any, contact tracing app will be endorsed, will reach the 60% adoption threshold is a hard sell considering a generally suspicious populace regarding data collection. In fact, there's a legislative movement in the US Congress to address public concerns by regulating automated contact tracing (https://healthitsecurity.com/news/congressional-bills-target-covid-19-contract-tracing-app-privacy).

**No Easy Cure**

The novel Coronavirus has presented us with new challenges on many fronts, some of which may be addressed by technology. One of those challenges may just be how we build trust into technology. The promise that comes with slowing the spread of an illness that has so disrupted our modern lives by simply installing an app should be a welcome innovation. Perhaps with time, assurances built into the technology by developers and bolstered by legislative efforts to protect the public, we'll see a reversal of what seems to be a missed opportunity for automated contact tracing. After all, technology responds.

**Please direct questions and inquiries about electronic discovery, computer forensics, cybersecurity and data analytics to info@digitalmountain.com.**

## UPCOMING INDUSTRY EVENTS

ABA 2020 ANNUAL MEETING, VIRTUAL
July 29, 2020 - August 4, 2020

BLACK HAT USA 2020, VIRTUAL
August 1-6, 2020

ILTACON 2020, VIRTUAL
August 24-27, 2020

TECHNO SECURITY & DIGITAL FORENSICS CONFERENCE
Myrtle Beach, SC: September 14-17, 2020

COMMERCIAL UAV EXPO AMERICAS, VIRTUAL
September 15-17, 2020

***Click here to see more upcoming events and links.***

*Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com. In the short term, she is available for webinars and remote e-conferences.*

**DIGITAL MOUNTAIN, INC.**
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

**www.digitalmountain.com**

***Contact us today!***

***FOLLOW US AT:***