BCLP. Client Intelligent

Insights

DESIGNING A FOURTH-AMENDMENT-FRIENDLY BLUETOOTH CONTACT TRACING APP IN THE UNITED STATES

May 01, 2020

SUMMARY

The quest to design a coronavirus contact tracing application in the United States using mobile devices' Bluetooth technology must take into consideration whether such an application would violate an individual's Fourth Amendment rights. This article discusses the best way to ensure that such an application does not run afoul of those important rights.

At the beginning of April, several news outlets began reporting that, following the partial lifting of statewide stay-at-home orders, the United States government would enter into private-public partnerships to develop contact tracing apps to prevent future surges in COVID-19 cases stemming from infections of the SARS-COV-2 novel coronavirus (the "**Coronavirus**"). In the middle of April, more specifics about these potential partnerships were revealed, including one potential partnership in which mobile operating systems developers ("**MOS Developers**") would provide applications for users' cell phones that would use their Bluetooth capabilities to perform contact tracing ("**Bluetooth Coronavirus Tracing Apps**" or "**BCTAs**"). The idea is essentially this: if a person tests positive for the Coronavirus ("**Patient Zero**"), and is quarantined, in order to prevent the spread of the disease by individuals who may have unwittingly picked it up from Patient Zero, various government health departments would be able to use information from Patient Zero's BCTA to download a roster of other devices whose Bluetooth was pinged by Patient Zero's due to proximity. The government would then use this information to:

- determine with whom Patient Zero had close contact over the prior several days before testing positive;
- contact those individuals and require that they submit to Coronavirus testing; and
- also quarantine any of those individuals who test positive (the "**Purpose**").

Using Bluetooth Coronavirus Tracing Apps in this manner would be a large step toward suppressing the infections of COVID-19 across the United States as portions of stay-at-home orders are lifted but before a vaccine for the illness is widely distributed. In order for BCTAs to become a reality though, they must be designed to survive any Fourth Amendment scrutiny that that information that the government collects therefrom does not constitute an "unreasonable search and seizure," contra individuals' constitutional privacy rights.

What is an "Unreasonable Search" and When Can the Government Nevertheless Use the Results.

An individual will have a claim against the government that their Fourth Amendment privacy rights have been violated[1] if they are subject to an unreasonable search or seizure of their property.[2] There are two general types of government activity that constitute a "search," and may be challenged as unreasonable: (i) an invasion of the reasonable expectation of privacy[3] and (ii) a trespass into a private area.[4]

Equally as important in the context of BCTAs are two sets of circumstances that the government may demonstrate that while an unreasonable search under the Fourth Amendment may have occurred, the government nevertheless can use the results thereof. The first occurs when the government uses information that an individual voluntarily turned over to a third party,[5] even if the individual gave the information to the third party for a purpose not connected to the government's use thereof (the "**Third-Party Exception**").[6] The second occurs when the government collects information for special needs, and the government's need for supervision and control outweighs the individual's reasonable expectation of privacy (the "**Special Needs Exception**").[7]

Of note, in the 2018 case *Carpenter v. United States*, the United States Supreme Court held that the Third-Party Exception did not apply to a week-long set of cell-site location information passively sent from a user's cell phone to nearby antennas of wireless providers, which the wireless provider then disclosed law enforcement to apprehend the user for a series of robberies.[8]

Additionally, as one commentator notes, the Special Needs Exception "is by far the least coherent and unsettled part of Fourth Amendment doctrine,"[9] owing to the weighing of facts in each case that is required for the government to demonstrate whether an exception for using the results of an unreasonable search occurred.

Designing a Fourth-Amendment-Friendly BCTA.

Given the jurisprudence, the optimal design for a BCTA that would survive Fourth Amendment scrutiny is revealed by answering the following questions: (i) does the government's use of location information through the BCTA constitute an "unreasonable search" and (ii) if so, is there an

exception that permits the government nonetheless to conduct the search and use the results thereof.

Based on what we know so far, a user would obtain a BCTA through one of two ways: downloading the BCTA from the MOS Developer's app store onto the user's mobile device or having the MOS Developer push the BCTA out to the user's mobile device. In either case, once downloaded, the BCTA could seek, or not seek, the user's consent to disclose their Bluetooth location for the Purpose.

In the scenario where the BCTA does not seek consent from a user to disclose their Bluetooth location information to the government for the Purpose ("**No-Consent Design**"), the Fourth Amendment analysis is triggered. First, the BCTA would likely be considered an invasion of the user's reasonable expectation of privacy because the user had no knowledge of the disclosure of their information. Furthermore, the No-Consent Design likely would not permit the government nonetheless to use the results of the unreasonable search (i) under the Third-Party Exception because the situation is too similar to the one in *Carpenter*, where the Third-Party Exception failed, and (ii) under the Special Needs Exception given the unsettled nature of the jurisprudence and the highly factual inquiry into whether the government's need for supervision and control outweigh the user's reasonable expectation of privacy.

With the No-Consent Design likely not surviving Fourth Amendment scrutiny, it is clear that any BCTA should therefore seek the consent of a user before the MOS Developer discloses their Bluetooth location information to the government for the Purpose ("**Consent Design**") to avoid the application of the Fourth Amendment. Ideally, the Consent Design would use an "opt-in" method. This author envisions a dialogue box that pops up on a user's screen the first time that they launch their BCTA, asking if the user consents to the disclosure of their Bluetooth location information to the government for the Purpose and giving the user the option to click "yes" or "no" to record their response. MOS Developers would then be permitted to share Bluetooth location information only from users who clicked "yes." Additionally, the Consent Design should include a setting to modify consent at any time, including the dates for which Bluetooth location information may be shared. This way, there would be no doubt at any point in time which users of the BCTA have agreed to have the MOS Developer disclose their Bluetooth location information to the government.

A Consent Design obviously may underreport potential Coronavirus infections if users choose not to opt in.[10] However, given that the government's collection of Bluetooth location information for the Purpose without consent likely would not survive Fourth Amendment scrutiny, a Consent Design that sidesteps the Fourth Amendment, would at least allow MOS Developers to roll out BCTAs as soon as possible as States begin to partially life stay-at-home orders.

---

1. Civil claims against the government for a violation of Fourth Amendment rights usually take the form of (i) an action in tort under the Federal Tort Claims Act or an action for the deprivation of constitutional rights under 18 U.S.C. § 1983, when the claim is against the federal government; and

(ii) an action in tort under the common law for the invasion of privacy, when the claim is against a state or local government.

2. *See* U.S. Const. amend. IV.

3. *See Katz v. United States*, 389 U.S. 347, 353, 360 (1967).

4. *See United States v. Jones*, 565 U.S. 400, 408 (2012).

5. *See Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).

6. *See United States v. Miller*, 425 U.S. 435, 443 (1976).

7. *See O'Connor v. Ortega*, 480 U.S. 709, 710 (1987).

8. *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018)

9. Rozenshtein, Alan Z., *Disease Surveillance and the Fourth Amendment*, Lawfare, April 7, 2020, https://www.lawfareblog.com/disease-surveillance-and-fourth-amendment

10. If a user has opted in to share their Bluetooth location information with the government, and if their BCTA pings the Bluetooth of a third party who does not have the BCTA or who has the BCTA but has not opted in, the government still could lawfully contact such third party and require them to submit to testing under the Fourth Amendment since the government would have probable cause to do so. *See e.g.*, *Illinois v. Gates*, 462 U.S. 213, 230-32 (1983).

RELATED CAPABILITIES

- Intellectual Property & Technology Disputes
- Regulation, Compliance & Advisory
- White Collar

MEET THE TEAM

Mark A. Srere

Washington

mark.srere@bclplaw.com
+1 202 508 6050
