IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ROBERT WRIGHT, JOHNNY KULA, KYLE DONNELL, JENNIFER HOHL, JANICE SANTELLO, AND ANDREW BLAKE,

Plaintiffs, on behalf of themselves and similarly situated others,

v.

MAURA HEALEY, in her official capacity as Governor of Massachusetts,

And

ROBERT GOLDSTEIN, in his official capacity as Commissioner of the Massachusetts Department of Public Health,

Defendants.

CASE NO: 3:22-cv-11936

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

CONSTITUTIONAL PROVISIONS

Plaintiffs oppose Defendants' Motion to Dismiss under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). Plaintiffs have adequately stated claims under the Fourth Amendment and the Fifth Amendment's Takings Clause; and Defendants' voluntary cessation of the MassNotify Program does not moot those claims.

REQUEST FOR ORAL ARGUMENT

Plaintiffs request oral argument to assist the Court in resolving the constitutional issues presented in this case.

INTRODUCTION

The Massachusetts Department of Public Health ("DPH") secretly installed without either consent or legal authority a software application called "Massachusetts Department of Public Health"[1] that sits (and will continue to sit) on over a million Android owners' devices. That application, referred to hereinafter as the "DPH App" or "App," was designed to collect personal and traceable location data about device owners to assist DPH's Covid-19 contact-tracing program, in clear violation of constitutionally protected privacy and property rights. The vast majority of Android owners are not even aware of this intrusion on their property and privacy interests. Defendants admits that neither they nor Google intend to uninstall it—rather they intend to keep all data the App transferred to the government in perpetuity on the unsubstantiated

[1] The actual name of the application appears to have changed over time. It was initially called "MassNotify." *See* Ron Amadeo, *Even Creepier COVID Tracking: Google Silently Pushed App to Users' Phones*, Ars Technica (June 21, 2021), available at https://arstechnica.com/gadgets/2021/06/even-creepier-covid-tracking-google-silently-pushed-app-to-users-phones/ ("There are two versions of the 'MassNotify' app on the Play Store. … A second version [is] labeled "v3" in the package name [and] has been slammed with negative reviews (1.1 stars as of publish time) with users alleging it was automatically installed on devices; some users even questioned if the app was malware.") (last visited June 12, 2023). By November 2022, the App was called "Massachusetts Department of Public Health" when viewed on an Android device. *See* screenshots at ECF 22, First Amendment Complaint 13.

assurance that such data is harmless. And they argue this Court should moot this action despite these ever-so-capable of repetition and ongoing violations of civil liberties.

The Court should reject Defendants' implausible and unsupported claim that DPH had nothing to do with shutting down an App that it developed and that bears the agency's name. *See* Def. Br. at 12. Rather, shutting down the App was "voluntary cessation," and Plaintiffs' claims are not moot under that exacting doctrine because they fail to make it "absolutely clear that the alleged wrongful behavior could not reasonably be expected to recur." *West Virginia v. EPA*, 142 S. Ct. 2587, 2607 (2022) (cleaned up). Moreover, Defendants received data that was allegedly unconstitutionally collected through the App. Def. Br. 9-10. Thus, the case is not moot when the Court can still provide relief by ordering deletion of the misbegotten data.

Defendants' arguments on the merits fare no better. They do not contest Plaintiffs' claim that secret installations of the App "are attributable to the Defendants." *Id.* at 14. Nor do they dispute that such installations constitute trespass and privacy invasions in violation of the Fourth Amendment. *Id.* at 15. Rather, they claim the DPH App does not gather information about device owners, *ibid*., which is contradicted by their admission to have received user data through the App, *id.* at 9-10. Defendants also contend surreptitious installations of unwanted software is not a Fifth Amendment taking because no one has a property interest in digital storage space on their privately owned mobile devices. *Id.* at 18. The Court must reject this untenable position because its adoption would extinguish tangible property rights for hundreds of millions of Americans. Finally, Defendants support their motion with an affidavit from an employee that asserts numerous facts regarding the merits of this case. *See* ECF 29-2, Affidavit of Dr. Catherine Brown ("Brown Affidavit"). Introducing ostensibly merits-based facts at the motion-to-dismiss stage—before

Plaintiffs may test them in discovery—is wholly inappropriate. The Court should not credit any of the Defendants' merits-based facts at this stage of the litigation.

STATEMENT OF FACTS

I. Factual Allegations

DPH relied on Google's application program interface ("API") to develop a software application for Android devices designed to assist DPH's Covid-19 contact-tracing program. ECF 22, First Amended Complaint ("FAC") ¶¶ 21, 25-28. The software uses Bluetooth signals to track other devices that come in close proximity and logs time-stamped Rolling Proximity Indicators ("RPI") on the Android device's system log. *Id.* ¶¶ 41-46. The App can send an exposure notification to those other devices if the owner reports infection with Covid-19. According to Defendants, this software was deployed as part of the MassNotify Program, which involved collaboration among DPH, Google, and other private entities not known to Plaintiffs when they filed the Complaint. These other entities included the Association of Public Health Laboratories ("APHL"), a nonprofit organization that worked on behalf of public health authorities around the country on Covid-19 responses.[2] Def. Br. 1.

In April 2021, DPH made an initial version of this software available for voluntary download by Android device owners on the Google Play Store, but few did so. FAC ¶¶ 25-27. DPH developed a new version, the DPH App at issue in this case, that was also available for voluntary download. But most downloads of the App were involuntary and occurred when DPH worked with Google to "automatically distribute[]" it starting in June 2021 to over one million

[2] APHL's role in the development of the software application at issue in this case is unclear. Google provided the API, and DPH is listed as the software's "developer." According to Defendants, APHL was involved in the management of data collected by the software application by offering its servers for use to state public health authorities, including DPH.

Android devices.[3] *See also* FAC ¶ 28. It was installed surreptitiously on the Android devices of over one million Massachusetts residents overnight, as well as out-of-state individuals who work in or travel through the Commonwealth, all without seeking their permission or even making them aware of it.

Defendants contend that the software at issue is not a downloadable "app" but merely a "setting" update. Def. Br. 4-5. This claim, however, is contradicted by the fact that the software is explicitly listed on Android devices as one of the "apps" installed, appearing alongside other apps such as "Maps" and "My Verizon." FAC at 13 (screenshots of Android devices). The DPH App was also available to be voluntarily downloaded on the Google Play Store as an "app." And it was referred to as an "app" by journalists, researchers, and commentators when it was first deployed.[4]

Numerous individuals who discovered the unwanted App on their Android devices, including Plaintiffs, were outraged at the invasion of their property and privacy. *See* FAC ¶¶ 34-35; *see also generally* Exhibit 1 to the FAC, ECF 22-1 (collecting subset of negative reviews). Others remain ignorant of the App on their devices because it does not appear as an icon on home screens. *Id.* ¶ 39. Many device owners did not—and still do not—know how to delete the App. *Ibid.* And even when some deleted it, DPH worked with Google to repeatedly reinstall it. *Id.* ¶ 38.

DPH worked with Google to secretly mass (re)install the DPH App to increase adoption of a tool designed to assist Massachusetts's then-ongoing Covid-19 contact-tracing effort. The App gathered massive quantities of time-stamped RPI information regarding each device's proximity to other Bluetooth-transmitting devices, and it placed that data onto each device's system log,

---

[3] Amadeo, *supra* note 1.

[4] *See, e.g.,* Amadeo, *supra* note 1; Abner Li, *Massachusetts 'MassNotify' Android App Auto-Installed, But COVID Exposure Alerts Are Not Enabled*, 9to5Google (June 19, 2021, 12:29 PM), available at https://9to5google.com/2021/06/19/massachusetts-massnotify-app/ (last visited June 8, 2023).

which DPH and others may access. A device owner's infection report to the App sends a notification to other devices that were recently in proximity to the infected device's owner. According to Defendants, DPH worked with APHL and other private entities to manage this data collection and processing. Def. Br. 8. APHL maintained and managed data collected by the App on behalf of DPH to obviate the need for DPH to build its own server system.[5]

Defendants assert the App anonymized RPI data. Def. Br. 9. But a study sponsored by the Department of Homeland Security concluded that contact-tracing apps developed using Google API—like the DPH App—failed to anonymize user identities. Joel Reardon, *Why Google Should Stop Logging Contact-Tracing Data*, AppCensus Blog (Apr. 27, 2021),[6] *cited at* FAC ¶¶ 49-50. It turns out the App logs personal identifiers of devices it comes into contact with, including their unique "MAC Addresses," alongside time-stamped anonymized RPI data onto the system log of the Android device on which the App is installed. *Ibid.* Some MAC Addresses are associated with Android devices owned by individuals and others are associated with readily identifiable fixed locations. *Ibid.* Any entity with access to that system log, which includes DPH and its private partners, can not only identify the owner of the device but also can then examine a timeline of all MAC Addresses he or she had been in proximity to, thereby inferring his or her movements—and associations. *Ibid.*

The DPH App takes up 15 megabytes of storage on an Android device. DPH claims the App does not function, and therefore does not log proximity information via Bluetooth transmissions, unless the device owner first turns it on. But Plaintiffs' and others' experiences call

[5] APHL Blog, *Bringing Covid-19 exposure notification to the public health community*, July 17, 2020, available at: https://www.aphlblog.org/bringing-covid-19-exposure-notification-to-the-public-health-community/(Last visited June 9, 2023).
[6] Available at: https://blog.appcensus.io/2021/04/27/why-google-should-stop-logging-contact-tracing-data/ (Last visited at June 9, 2023).

that claim into question. Plaintiffs Donnella and Santello usually keep their Bluetooth off but repeatedly found their devices' Bluetooth transmitting without their awareness when the App was installed but not turned on. FAC ¶ 57. Other users have likewise complained that the App causes their devices to transmit via Bluetooth without their permission, even when the App was not turned on. *Id.* ¶ 57 n.45.

Plaintiffs filed a class-action lawsuit on November 22, 2022, and amended their Complaint on March 23, 2023. The Amended Complaint alleges that Defendants violated their Fourth Amendment rights by secretly installing the unwanted App on their Android devices, and thereby gathered private information about them. FAC ¶¶ 77-86. Plaintiffs also allege that secret installation of the unwanted App is an uncompensated taking of digital storage space, in violation of the Fifth Amendment. *Id.* ¶¶ 87-95. They request declaratory and injunctive relief requiring Defendants to stop installing the App; to remotely remove the App from devices; and to delete data amassed through the App. *Id.* at 31.

II. Additional Facts Defendants Attempt to Introduce

Defendants have submitted the affidavit of one of their employees, Dr. Catherine Brown, to introduce a number "Additional Facts." Def. Br. 8 (citing Brown Affidavit). A few facts are subject to judicial notice, such as MassNotify ending in May 2023, and the DPH App being taken off the Google Play Store. Other factual assertions, however, improperly dispute allegations of the Amended Complaint on the merits. Dr. Brown presents a competing account of the MassNotify Program, the technical functionality of the DPH App, and DPH's technical capabilities. Brown Affidavit ¶¶ 4-7. She also identifies private partners that DPH worked with in managing data collected by the App, including Google and APHL, and describes the relationship and communications with those partners. *Id.* ¶¶ 5, 7-10. While she confirmed Plaintiffs' allegation that

DPH received data from the App, she claims that such data "did not include any personal or location information" and further asserts that DPH "does not have, and has never had, access to personalized data … via MassNotify." *Id.* ¶¶ 12-15.

Some of Dr. Brown's assertions are clearly inadmissible as conjecture or hearsay. For instance, she asserts that DPH is not aware of any plans by APHL to bring back servers used to process data for the App without providing a foundation for her awareness of APHL's plans. *Id.* ¶ 9. *See* Fed. R. of Evid. 602. Her description of the DPH App's functionality is entirely "[b]ased on representations by Google, Apple APHL and other partners," and she relies on "representations made by Google" to assert that Google lacks the technical capability to remotely uninstall the App "without initiating a system-wide update." *Id.* ¶¶ 5, 10. *See* Fed. R. Evid 801(c).

Dr. Brown further asserts that "DPH … does not have any *present* intention or capacity of starting another digital exposure notification system." *Id.* ¶ 9 (emphasis added). But she makes no assurances regarding DPH's future intentions to start another system. Nor does she make any assurances regarding DPH's ability to acquire the capacity to do so, either on its own, or through partnering with ostensibly private entities. Plaintiffs have not had a chance to examine any of Dr. Brown's assertions, so Plaintiffs dispute her factual assertions until they have an opportunity for discovery, including by taking her deposition.

STANDARD OF REVIEW

In resolving a Rule 12(b)(6) motion, the court must "take the complaint's well-pleaded facts as true, and [it must] draw all reasonable inferences in the plaintiffs' favor." *Lowe v. Mills*, No. 22-1710, -- F. 4th -- 2023 WL 3642081, at *4 (1st Cir. May 25, 2023) (cleaned up). "At this stage, [the Court] ordinarily may only consider facts alleged in the complaint and exhibits attached thereto, although [it] may also consider materials fairly incorporated in the complaint or subject to

judicial notice." *Ibid.* (cleaned up). The Court may not consider facts introduced via an affidavit from Defendants' employee that disputes facts at issue in the case. Such factual assertions are not properly before the Court until trial.

The same standard applies to a Rule 12(b)(1) motion to dismiss for lack of subject-matter jurisdiction: "the district court must construe the complaint liberally, treating all well-pleaded facts as true and indulging all reasonable inferences in favor of the plaintiff." *Aversa v. United States*, 99 F.3d 1200, 1210 (1st Cir. 1996). Moreover, when deciding Article III jurisdiction, the Court must "accept as valid the merits of [Plaintiffs'] legal claims." *FEC v. Cruz*, 142 S. Ct. 1638, 1647 (2022). While a court may consider jurisdictional facts outside the pleading, including an affidavit submitted by Defendants' employee, the "Court must 'defer resolution of the jurisdictional issue until the time of trial' unless [that] affidavit places the material facts beyond genuine dispute." *Barrett v. QuoteWizard.com, LLC*, No. CV 20-11209-LTS, 2020 WL 7626464, at *6 (D. Mass. Nov. 12, 2020) (quoting *Valentin v. Hosp. Bella Vista*, 254 F.3d 358, 363 n.3 (1st Cir. 2001)). Deferring the resolution of disputed jurisdictional facts is especially appropriate where such facts "are inextricably intertwined with the merits of the case." *Valentin*, 254 F.3d at 363 n.3. Otherwise, a defendant could disguise merits-based facts as "jurisdictional" to improperly contest claims on the merits, thus circumventing the requirement for the Court to "accept as valid the merits of … claims" during jurisdictional analysis. *See Cruz*, 142 S. Ct. at 1647. Courts may also order discovery on disputed jurisdictional facts. *See New England Coll. v. Drew Univ.*, No. CIV. 08-CV-424-JL, 2009 WL 395753, at *4 (D.N.H. Feb. 17, 2009).

ARGUMENT

I. THE END OF MASSNOTIFY DOES NOT MOOT THIS CASE

"The burden of establishing mootness rests squarely on the party raising it, and the burden is a heavy one." *Mangual v. Rotger-Sabat*, 317 F.3d 45, 60 (1st Cir. 2003) (cleaned up). The Court should take a "claim-by-claim approach." *Smith v. Becerra*, 44 F.4th 1238, 1247 (10th Cir. 2022). "A claim is moot only if no relief is available." *Kuperman v. Wrenn*, 645 F.3d 69, 73 (1st Cir. 2011) (citing *Church of Scientology of Ca. v. U.S.*, 506 U.S. 9, 12 (1992)). Here, Plaintiffs' Fourth Amendment claim is not moot because the Court may order relief by requiring DPH to delete data its App collected unlawfully. *See Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 338 (4th Cir. 2021). The Court may also grant requested relief by ordering DPH to work with Google to remotely remove the App from devices on which it was installed without permission. Moreover, DPH merely disclaimed a "present intention" of not restarting the same or similar program; it made no promise about future action. Def. Br. 9. Defendants thus failed to make it "absolutely clear that the alleged wrongful behavior could not reasonably be expected to recur," so mootness is also inappropriate under voluntary-cessation and repetition-yet-evading-review doctrines. *West Virginia*, 142 S. Ct. at 2607 (cleaned up); *see also Kingdomware Techs., Inc. v. U.S.*, 579 U.S. 162, 170 (2016).

A. The Case Is Not Moot When the Department Retains Unlawfully Collected Data

A challenge against a governmental surveillance program is not moot simply because the program ends, if the government retains data unlawfully collected through that program. In *Beautiful Struggle*, 2 F.4th at 338, Baltimore ended an aerial surveillance program and said it had "no intention of accessing the data [from the program] to track and potentially identify individuals." *Ibid.* The *en banc* Fourth Circuit held the case was not moot because Baltimore still

retained the data and thus "might access" and "could access … data collected by alleged unconstitutional means" for non-tracking purposes. *Ibid.* In *Church of Scientology*, the Supreme Court likewise held that a challenge against unlawful collection of data by the government is not moot unless that data was "either returned or destroyed." 506 U.S. at 15.

Here, Plaintiffs allege that DPH unconstitutionally collected data about them by working with private entities to secretly install and operate the DPH App. FAC ¶¶ 62-66, 77-86. Defendants concede that DPH received data collected through the App from those entities. Def. Br. 9-10 (citing Brown Affidavit ¶¶ 12-15). Defendants' contention that none of the data DPH received or has access to "include any personal or location information," *id.* at 9, is a factual assertion contesting the merits of Plaintiffs' Fourth Amendment claim. Because the Court must accept the merits of Plaintiffs' claim when analyzing Article III jurisdiction, *Cruz*, 142 S. Ct. at 1647, it must reject Defendants' characterization of the data as being lawfully collected or otherwise harmless. Rather, the Court must assume the data retained by DPH was collected unconstitutionally for the purpose of jurisdictional analysis. *Ibid.* Despite MassNotify's cessation, the Court may still provide relief by ordering DPH to destroy any unlawfully collected data or otherwise enjoin DPH from accessing such data; therefore, the case is not moot. *Church of Scientology*, 506 U.S. at 15; *Beautiful Struggle*, 2 F.4th at 337.

B. The Case Is Not Moot Because the Court Can Order the App's Remote Removal

Plaintiffs request that the Court order DPH to work with Google to remotely remove the App from all devices. FAC at 31. Defendants' sole argument for why this relief is not possible is their contention that "[b]ased on representations made by Google to the Department, Google also does not have this technical capability [to remotely remove the App] without initiating a system-wide update on all Android devices." Def. Br. 9 (citing Brown Affidavit ¶ 10). This statement is

inadmissible hearsay because "its probative value ultimately depends on the truth of [Google's] unsworn out-of-court utterance." *Noviello v. City of Bos.*, 398 F.3d 76, 85 (1st Cir. 2005).[7] Additionally, even if true, Defendants fail to carry their burden to explain why remote removal through a system-wide update is not possible. The Court therefore can still grant Plaintiffs' requested relief, and the case is not moot.

C. The Case Is Not Moot Under the Voluntary-Cessation Doctrine

Under the voluntary-cessation doctrine, the government's decision to end challenged conduct "does not moot a case unless it is absolutely clear that the allegedly wrongful behavior could not reasonably be expected to recur." *West Virginia*, 142 S. Ct. at 2607 (cleaned up). Defendants argue that the doctrine does not apply by implausibly asserting that the Massachusetts Department of Public Health somehow had nothing to do with withdrawing an App called "Massachusetts Department of Public Health"[8] or with ending a public-health surveillance program called "MassNotify." Def. Br. 12. While Defendants rely (often improperly) on the Brown Affidavit, it is noteworthy that they cited neither that Affidavit nor any other factual authority in contending that "[t]he Department did not participate in this decision [to withdraw the App] and did nothing to hasten the shutdown of MassNotify." *Ibid.* In other words, the claim DPH had nothing to do with ending MassNotify is an unsupported and self-serving assertion that the Court may not accept for this Rule 12(b)(1) motion.

Defendants' assertion that DPH had nothing to do with ending MassNotify is also "inextricably intertwined with the merits of the case" and thus may not be resolved at this stage. *Valentin*, 254 F.3d at 363 n.3. Plaintiffs allege the installation and operation of the DPH App are

[7] For the same reason, all of Dr. Brown's assertions "[b]ased on representations made [to her] by Google, Apple, APHL, and other partners" are inadmissible hearsay. *See* Brown Affidavit ¶ 5.
[8] *See* FAC at 13 (screenshots).

state action because actions taken by private partners with respect to the App are attributable to Defendants. FAC ¶¶ 62-63.[9] Defendants acknowledge that the Court should "assum[e] for this motion that [such] actions … are attributable to the Defendants." Def. Br. 14. Defendants' self-contradictory assertion—especially without factual foundation—that the decisions to end MassNotify and withdraw the DPH App somehow are *not* attributable to DPH must be rejected here and tested in litigation.

The Court instead must attribute the end of MassNotify to DPH and apply the voluntary-cessation doctrine. Defendants cannot meet the "heavy burden" required for mootness under that doctrine because their contention that DPH has no "present intention" of redeploying the App, Def. Br. 9 (citing Brown Affidavit ¶ 9), falls far short of "absolute[]" confirmation that the challenged policy will never be "reimpose[d]." *West Virginia*, 142 S. Ct. at 2607.

Defendants claim that the decision to end MassNotify occurred in February 2023, in response to the then-anticipated end of the federal public health emergency, which was based on falling Covid-19 fatality rates. *See* Brown Affidavit ¶ 8. But new and more virulent variants of Covid-19 may yet emerge—as has happened multiple times already over the past several years. Indeed, the weekly Covid-19 fatality rate in February 2023 is approximately the same as that of Spring 2021, right before a new and more deadly strain emerged in Summer 2021 that motivated DPH to widely deploy the App.[10] Defendants cannot possibly guarantee that no new Covid-19 strains or other contagious diseases will ever emerge that could motivate DPH to again partner

[9] While the Amended Complaint did not explicitly name APHL and other private partners of DPH, the Court must "construe[ ] … liberally," *Aversa*, 99 F.3d 1200, 1210, Plaintiffs' state-action allegations to encompass these other private partners previously unknown to Plaintiffs.

[10] CDC, *COVID Data Tracker: Daily and Total Trends*, https://covid.cdc.gov/covid-data-tracker/#trends_weeklydeaths_select_00 (last visited June 8, 2023).

with private entities to secretly and forcibly install the DPH App in violation of Plaintiffs' Fourth and Fifth Amendment rights.

The threat of recurrence is even greater for Plaintiffs' Takings claim. Regardless of an app's surveillance capabilities, Plaintiffs argue that the government may not forcibly install *any* unwanted software onto people's personal electronic devices—thereby taking up valuable digital storage space—without just compensation. FAC ¶ 87-95. Just as in *West Virginia*, "the Government nowhere suggests that if this litigation is resolved in its favor, it will not" ever forcibly install unwanted software on private electronic devices without just compensation. 142 S. Ct. at 2607 (cleaned up). "[I]ndeed it vigorously defends the legality of such an approach," *ibid.* (cleaned up), by insisting individuals have no property interest in the digital storage space of privately owned electronic devices. *See* Def. Br. 18. Courts must "not dismiss a case as moot in such circumstances." *West Virginia*, 142 S. Ct. at 2607.

D. The Case Is Not Moot Under the Repetition-Yet-Evading-Review Doctrine

The end of challenged conduct also cannot moot a case when that conduct is "capable of repetition, yet evading review." *Kingdomware Tech., Inc. v. United States*, 579 U.S. 162, 170 (2016). This doctrine applies where "(1) the challenged action is in its duration too short to be fully litigated prior to cessation or expiration, and (2) there is a reasonable expectation that the same complaining party will be subject to the same action again." *Ibid*. (cleaned up). The first condition is easily met because "two years is too short to complete judicial review of the lawfulness" of challenged conduct. *Ibid*. Even if Plaintiffs filed their case in June 2021, when DPH began to illegally install the DPH App, the challenged conduct would still be capable of evading review.

The second condition is not exacting and does not require "repetition of every 'legally relevant' characteristic." *FEC v. Wis. Right to Life*, 551 U.S. at 449, 463 (2007).[11] It is satisfied if government officials "retain[ed] authority to reinstate" the challenged policy. *Tandon v. Newsom*, 141 S. Ct. 1294, 1297 (2021) ("[E]ven if the government withdraws or modifies a COVID [policy] in the course of litigation, that does not necessarily moot the case."). Defendants can easily work with private actors such as Google and APHL to redeploy the DPH App that violates Plaintiffs' Fourth Amendment rights. DPH did so in 2021 and Defendants present no reason why the agency cannot do so again in response to a new Covid-19 strain or another contagion. Unless stopped in this case, Defendants would retain authority to forcibly install any other unwanted software without just compensation, either on its own or by coopting private entities, including entities other than Google and APHL. Plaintiffs' Fourth Amendment and Takings Clause injuries are capable of repetition, yet evading review, and thus are not moot.

E. In the Alternative, Plaintiffs Request Jurisdictional Discovery on the Brown Affidavit

Defendants assert numerous "Additional Facts" from the Brown Affidavit to support their jurisdictional argument. Def. Br. 8-11. Aside from the end of MassNotify in May 2023, Plaintiffs dispute Dr. Brown's factual assertions until they have an opportunity for discovery, including deposing her. This includes discovery on the DPH App's technical functionality; DPH's relationship (including communications) with Google and other private partners with respect to developing, installing, and operating the App; DPH's discussions with its private partners

[11] Defendants' request to dismiss the Governor is inappropriate, *see* Def. Br at 14, because Plaintiffs' Takings claim is not limited to uncompensated takings due to forcibly installation of unwanted software *by DPH*. Because repeat unlawful conduct does not require "repetition of every 'legally relevant' characteristic," *Wis. Right to Life*, 551 U.S. at 463, Plaintiffs' Takings claim fairly encompasses uncompensated installation of unwanted software by *any* Commonwealth agency. Hence, it is appropriate to keep the Governor in the case.

regarding ending the MassNotify program; DPH's capability to remove the App remotely and/or redeploy the App in the future on its own or in concert with private actors; the characteristics of all data DPH received or had access to through the App, either on its own or through private actors.

Again, the Court should reject the Brown Affidavit's disputed facts at the motion-to-dismiss stage as being inextricably intertwined with the merits of Plaintiffs' claims, which must be accepted as valid for the purpose of jurisdictional analysis. *Cruz*, 142 S. Ct. at 1647. In the alternative, Plaintiffs request jurisdictional discovery. Because the Brown Affidavit's factual assertions are so wide-ranging and intertwined with the merits of the case, jurisdictional discovery as to those facts will be largely indistinguishable from discovery in advance of trial.

II. PLAINTIFFS HAVE STATED CLAIMS UPON WHICH RELIEF MAY BE GRANTED

A. Installation and Operation of the App Constitute State Action

Defendants acknowledge that, for the purposes of their motion, actions taken by private entities such as Google with respect to the DPH App "are attributable to the Defendants." Def. Br. 14. They do not dispute Plaintiffs' allegation that DPH cooperated with Google to develop the App and install it secretly across the Commonwealth to serve DPH's purpose. *See* FAC ¶¶ 63-66. Nor would it have been possible to do so. DPH was listed as the App's developer; and the App was called "Massachusetts Department of Public Health." *Id.* at 13 (screenshots). The App is clearly DPH's software and not merely some sort of Google "setting" update. Google would not have secretly installed government-developed and government-owned software onto millions of Android devices without close coordination with DPH. There are more than enough "clear indices of Government's encouragement, endorsement, and participation" to conclude that surreptitious

installations of the App were state action. *Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602, 614 (1989).

APHL likewise is a state actor to the extent it managed and processed data collected by the DPH's App on DPH's behalf. APHL's own blogposts confirm that it was acting on behalf of "state and territorial public health agenc[ies]" to support each contact-tracing "app developed by [a] public health agency."[12] These admissions confirm that APHL's services were state action.

B. Plaintiffs Have Stated a Claim for Violation of the Fourth Amendment

The Fourth Amendment, which applies to the Commonwealth through the Fourteenth Amendment, protects "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures." U.S. Const. amend. IV. DPH conducted property-based searches by trespassing onto Plaintiffs' private property—their Android devices—to install an App that gathers information about them by collecting time-stamped data regarding their proximity to other Bluetooth-transmitting devices, whether fixed or mobile. *See Taylor v. City of Saginaw*, 922 F.3d 328, 332 (6th Cir. 2019) (citing *U.S. v. Jones*, 565 U.S. 400, 404-05 (2012)). It also conducted privacy-based searches because the RPI data and MAC Addresses collected by DPH's App creates an "all-encompassing record" of owners' whereabouts. *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018). These warrantless searches were not reasonable.

Defendants do not contest that DPH's installation of the App violated Plaintiffs' reasonable expectation of privacy and constituted a trespass. Def. Br. 15 ("Setting aside the first two questions (reasonable expectation of privacy and trespass) for this motion"). Rather, they contend Plaintiffs "have not alleged any facts plausibly showing that the Department or the Commissioner attempted

[12] APHL Blogpost, supra note 5.

to obtain information about individual Android users through the [App]." *Ibid.* But this assertion is contradicted by Defendants' own admission to have received data through the App. *Id.* at 9-10. While they claim that such data do not reveal personal information, *ibid*., that is a factual claim to be tested in discovery, not to be decided in Defendants' favor at the motion-to-dismiss stage. They nonetheless muster three meritless arguments in support of their improper factual assertion.

First, although Defendants concede that DPH cooperated with Google to install the App such that Google's acts were "attributable to Defendants," *id.* at 14, they insist that such cooperative installations were not done "for the purpose of gathering information about [Android device owners]," *id.* at 15. Rather, Defendants say DPH worked with Google "to increase participation in the Commonwealth's digital exposure notification system." *Ibid.* But Defendants' motive is irrelevant. Besides, that notification system explicitly relies on gathering information about Android device owners, *i.e.*, collecting time-stamped data on their proximity to other Bluetooth-transmitting devices. Thus, the secret installations were motivated by the desire to increase adoption of DPH's information-collecting App.

Second, Defendants argue that "the very documents upon which [Plaintiffs] rely in framing their complaint flatly refute … claims" that DPH and others may "access device logs that allegedly contain (MAC Address) information … that could be analyzed to reveal the device owners' movements and associates." *Id.* at 16. But instead of identifying these "very documents" that supposedly refute Plaintiffs' claims, Defendants merely cite a four-page section of *their own* brief. *Ibid.* (citing *id* at 5-8).[13] In any event, Plaintiffs' documents support their claims. In particular, the

[13] The four-page section of Defendants' brief refers to a document cited in the Amended Complaint in which Google asserts that "[n]o GPS or location information from [a user's] phone will ever be collected or used by" contact-tracing apps developed using Google-provided API. Def. Br. at 6 (quoting Google documented cited at FAC ¶ 41. n.37). But that assertion is irrelevant because

Reardon Study, cited at FAC ¶¶ 49-50, analyzed contact-tracing apps developed through Google's API to conclude that:

> An entity that collects users' logs can turn the RPI they hear [through the App] into the corresponding MAC address; with access to existing [public] databases, they can turn the MAC address into a geolocation. This allows [the entity] to learn a location history of a user based on geolocating the RPIs they hear.

Documents cited in the Amended Complaint indisputably support Plaintiffs' contention that DPH's App collects data that could be used to geolocate devices on which it is installed.

Third, Defendants argue that "Plaintiffs do not allege that the Commissioner actually accessed those system logs, reviewed the MAC Addresses, or otherwise tracked android device owners[.]" Def. Br. 16. But Plaintiffs were not required to plead that the Commissioner or any specific person accessed their data or tracked them. Rather, it is sufficient to plead that the government "collected by allegedly unconstitutional means" data that it "could access," even for non-tracking purposes. *Beautiful Struggle*, 2 F.4th at 337. Plaintiffs clearly alleged that "the Contact Tracing App gives DPH access to system logs of Android devices on which the App is installed." FAC ¶ 52. And the Reardon Study shows how DPH or its private partners could use that log to geolocate users. *Id.* ¶ 49-51.

C. Plaintiffs Have Stated a Fifth Amendment Takings Claim

The Fifth Amendment's Takings Clause, which applies to the Commonwealth through the Fourteenth Amendment, provides that "private property [shall not] be taken for public use, without just compensation." U.S. Const. amend. V. A physical occupation of property is a *per se* taking,

---

Plaintiffs' Fourth Amendment claim is not based on the collection of *GPS* data, but rather on the collection of MAC Address data that are logged alongside RPI data, which could be used to geolocate users. FAC ¶¶ 51-57. Moreover, as the Amended Complaint explained, Defendants cannot with a straight face rely on Google's promise of being "privacy-focused" when the Commonwealth recently sued Google for violating its own privacy-protection promises and obtained $10 million of a $392 million settlement. *Id.* ¶ 59, 61.

even if it "has only minimal economic impact on the owner," *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 434 (1982), or if such occupation is only temporary. *Cedar Point Nursery v. Hassid*, 141 S. Ct. 2063, 2066, 2072 (2021). By installing an unwanted App on Plaintiffs' Android devices, DPH took 15 megabytes of digital storage from more than one million device owners without just compensation.

Defendants respond that Plaintiffs lack a property interest in the digital storage space of their Android devices. Def. Br. 18. If true—and it is not—that would be an unwelcome surprise to hundreds of millions of Americans who own electronic devices. Defendants' assertion that "[t]here are no underlying factual allegations that Plaintiffs exclusively own this storage space," *id.* at 18, ignores the indisputable fact that each Plaintiff exclusively owns his or her Android device, and by extension the storage that comes with it.[14] *Cf. Riley v. California*, 573 U.S. 373 (2014) (suspect's property interest in digital data stored in a cell phone requires issuance of a warrant before data could be searched by police).

Nor do Plaintiffs lack a property interest simply because, as Defendants contend, Google has the capacity to automatically install the App. Def. Br. 18. The installation of the App was unlawful—the fact that an entity has the capacity to intrude onto property does not somehow vitiate the owner's property interest. Moreover, Google's contractual rights to install software updates on Plaintiffs' devices are analogous to tenants' being able to come and go in Loretto's apartment

[14] There is nothing special to differentiate digital storage from traditional storage spaces such as the apartment in *Loretto*. While invisible to the human eye, digital storage is still composed of electrons that have mass, and thus are not somehow less "physical" than traditional spaces. *See, e.g.*, Venkatesh Vaidyanathan, *Does Digital Data On Your Hard Disk Have Mass?*, Science ABC (July 8, 2022), available at: https://www.scienceabc.com/eyeopeners/does-the-digital-data-on-your-hard-disk-have-mass.html (last visited June 12, 2023) ("Yes, the digital data on your hard disk has mass."). And digital storage has tangible monetary value. Individuals pay more for electronic devices that have greater digital storage capacity. They also pay for alternative forms of storage when the space on their devices runs out.

pursuant to leasing agreements. But such rights do not extend to installing an unwanted government-developed app at a government agency's behest.[15]

Defendants next argue that no taking occurred because Plaintiffs could delete the App and thus there was no "required acquiescence." Def. Br. 19 (quoting *FCC v. Florida Power Corp*., 480 U.S. 245, 252 (1987)). But deletion is possible only if a device owner becomes aware of the App's presence. Given the stealthy nature of the App's installation, most device owners were not aware and thus could not delete it. FAC ¶ 39. Four of the Plaintiffs in this case were not aware of the App on their devices until November 2022, over one year after MassNotify began in June 2021. *Id.* ¶ 3-6. Additionally, DPH could simply reinstall the App if it was deleted—and did so repeatedly. *Id.* ¶ 38. Plaintiffs thus had no way of definitively excluding the App from their devices even after they had become aware of it. They have been at the mercy of the App's occupying their devices whenever DPH wants to reinstall it. *See Cedar Point*, 141 S. Ct. at 2066 (recognizing periodic and temporary occupations violate the Takings Clause).

CONCLUSION

The United States Constitution guarantees that citizens will be secure in their property against unreasonable intrusions by the government and that such property cannot be taken by the government by fiat as was done here. What's more, the fruits of those unconstitutional intrusions cannot be held at all, much less in perpetuity, by the government. The Court should deny Defendants' motion to dismiss under Rules 12(b)(1) and 12(b)(6). In the alternative, Plaintiffs request jurisdictional discovery.

[15] If Google advertised such terms in its user agreement, its customer base might shrink dramatically.

June 12, 2023

Respectfully submitted,

/s/ *Sheng Li*
Sheng Li, *pro hac vice*
sheng.li@ncla.legal
Margaret A. Little, *pro hac vice*
peggy.little@ncla.legal
NEW CIVIL LIBERTIES ALLIANCE
1225 19th St. NW, Suite 450
Washington, DC 20036
Telephone: 202-869-5210

Thomas H. Curran, BBO# 550759
tcurran@curranantonelli.com
Peter Antonelli, BBO# 661526
pantonelli@curranantonelli.com
CURRAN ANTONELLI, LLP
Ten Post Office Square, Suite 800 South
Boston, MA 02109
Telephone: (617) 207-8670
Fax: (617) 850-9001

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on June 12, 2023, an electronic copy of the foregoing was filed electronically via the Court's ECF system, which effects service upon counsel of record.

*/s/*Sheng Li
Sheng Li