UIA International Association of Lawyers

Technology, Tracing & Telemedicine:
Privacy, Risks and Benefits

COVID Contact Tracing:
Progress or Privacy at the Crossroads?

Janice F. Mulligan

Mulligan, Banham & Findley

www.janmulligan.com

mulligan@janmulligan.com

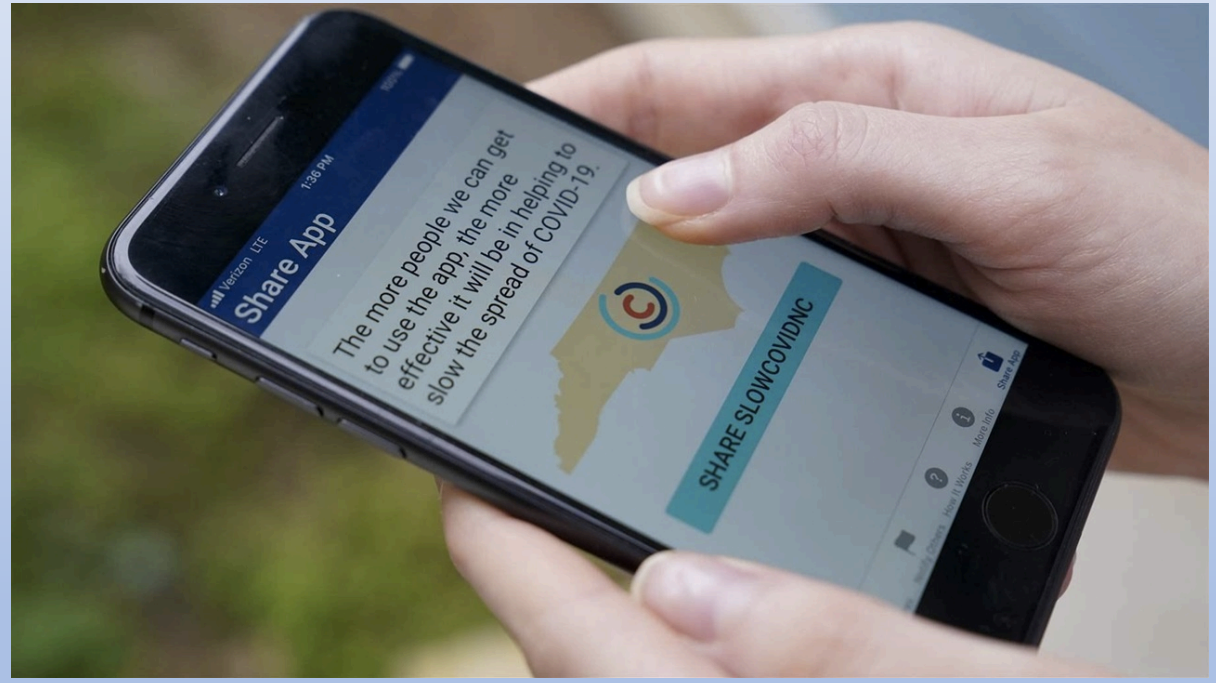
San Diego, California USA

The plan: Use existing technology to create phone apps to track COVID diagnoses and exposure through an

Exposure notification system (ENS)

Spring 2020: Google and Apple create joint effort to provide government health departments with tools to build these apps for their communities

***The Goal*:** Use ENS to slow or even stop coronavirus transmission



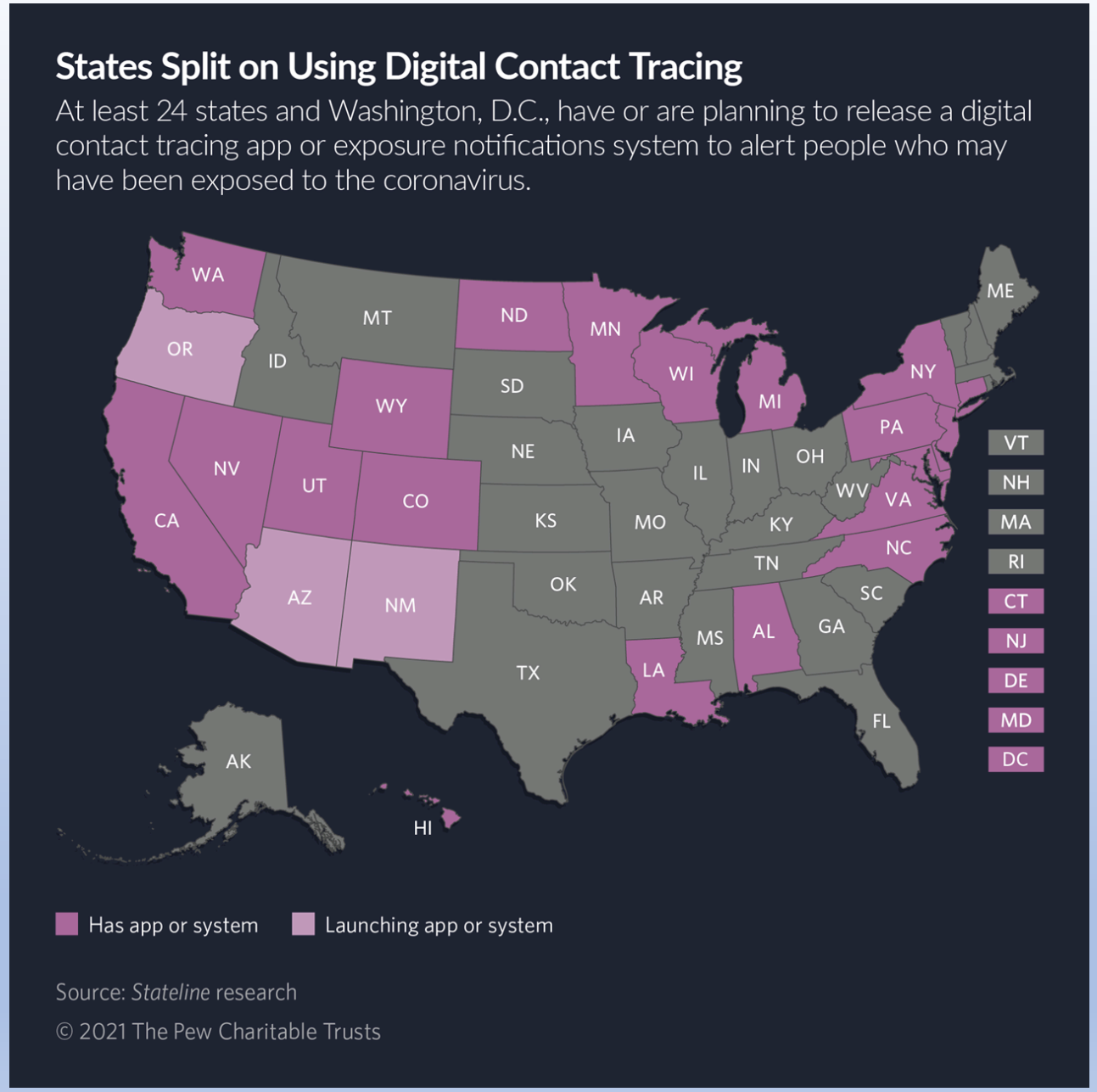
What happened?

The Google and Apple ENS is in use in 37 countries

A February 2021 report from the **United Kingdom** estimates alerts from the app helped to **prevent approximately 600,000** coronavirus cases since September 2020

A peer-reviewed January study of the app's use in **Spain** last summer determined the app **identified nearly twice as many COVID-19 exposures as human contact tracers**

For States' COVID Contact Tracing Apps, Privacy Tops Utility, **Pew Trust Stateline** March 19, 2021
https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/19/for-states-covid-contact-tracing-apps-privacy-tops-utility



24 U.S. states developed and promoted Apple and Google-based ENS apps

>28 million people in the United States downloaded the ENS mobile apps or activated exposure notifications on their smartphones

Why do some U.S. states refuse to make an ENS tracing app?

- One in five U.S. adults don't own a smartphone. Ohio State's decision not to make an ENS app **balanced equity concerns** because a person without a smartphone might make them vulnerable without access.

- Mississippi and Texas cited **privacy and accuracy concerns** in deciding not to use ENS.

- Citing privacy concerns, South Carolina **halted ALL ENS tracking** efforts by passing a bill ***forbidding*** health officials from using contact-tracing apps on cellular devices.

What are the Safeguards to ENS Privacy Concerns?

- Bluetooth-based setup is **voluntary & opt-in only**

- The app is allegedly **anonymous**

- Only public health authorities can activate system

- **Codes change regularly**

- People are not told where or by whom they were exposed to the virus

WHAT DATA
Is At Greatest Risk of Being Collected?

"Associated encrypted metadata":

- When individuals notified via app that they have the virus, their **individual IP address and other metadata is detectable *by app server***

- Exposed individuals may elect to upload their **own unique identifiers** warning those with whom they have been in contact

Apple and Google require that apps "promise" not to collect and retain this information….

What will happen to all of this data after the pandemic is over?

The risk of 'function creep' and use of data for *purposes unintended by the data subjects*

In China, where Alipay and WeChat also host COVID tracing apps, those companies assert contractual rights to keep the data

Apple and Google **have reserved functionality for additional unspecified associated metadata that might be collected!**

COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes Bradford *et al* Journal of Law and the Biosciences, 28 May 2020

Risk:
What if ENS information is collated with other data?

Apple & Google say their system is designed to make automated collection of this collated data usage "**prohibitively difficult**".

However, those who administer apps using the system can ***collect some of this information separately*** at the time of diagnosis or exposure notification.

A combination of exposure data collected by apps **with individual user identities and location data separately collected exposes users to potential identification.**

How could this happen?

BIG DATA:

Smartphone data. GPS tracking. Security cameras. License plate readers. Drones.

Potential for collation of *combined* data

= Multi-intelligence or Automated Fusion

Historically, data was cumbersome and difficult to correlate, creating a natural protection against total surveillance

Now, using "**correlation engines,**" a suite of algorithms can sift through massive data **looking for patterns and connections**

With the click of an Investigate button, our scattered digital footprints may become a **single unified file on our lives**

The risk is real….

Tech giants Cisco, Microsoft, and Motorola sell **fusion systems globally**

Palantir counts among its clients the U.S. Central Intelligence Agency **(CIA)**, Immigration and Customs Enforcement **(ICE),** and ***the Centers for Disease Control and Prevention (CDC)***

Correlation engines ***acquire privately owned libraries of smartphone location***

For example, the Pentagon's Special Operations Command has many such libraries, *including those from a Muslim prayer app with tens of millions of users*

The goal is to combine libraries of data to create a "**continuously updated digital chessboard"**

ARTHUR HOLLAND MICHEL,
Eyes in the Sky: The Secret Rise of Gorgon Stare and How It Will Watch Us All

In the US there are no specific national laws governing fusion technology

Absent a legal challenge to test its constitutional integrity, **there's little to prevent merging blended data sets**, even if doing so might generate information that investigators would otherwise have needed a court order to obtain

Laws must be found to protect this data if the ENS data is to be kept from being swept up into the fusion technology library

U.S. Has No Federal Privacy Laws to Protect Data Taken from ENS Apps

Doesn't HIPAA apply to the ENS App?

HIPAA applies **only** to *data collected by health providers* or businesses hired by providers to process their data

An individual's COVID diagnosis from a lab would be subject to HIPAA's Privacy Rule, **but an ENS app may be *beyond the scope of HIPAA.***

As long as it is the individuals themselves who disclose information to the ENS App, and not the health provider directly, HIPAA may not apply to an ENS system.

COVID-19 contact tracing apps: a stress test for privacy and data protection Bradford, et al., *Journal of Law and the Biosciences*, Volume 7, Issue 1, May 2020
https://academic.oup.com/jlb/article/7/1/lsaa034/5848138

No liability under U.S. FDA or FTC for ENS app:

COVID Contact Tracing Apps are **not** **considered “medical devices”**

Digital Health Policies and Public Health Solutions for COVID-19 ***FDA's Digital Health Policies Allow Innovators to Create COVID-19 Related Public Health Solutions https://www.fda.gov/medical-devices/coronavirus-covid-19-and-medical-devices/digital-health-policies-and-public-health-solutions-covid-19***

What about state privacy laws?

- **U.S. state laws are all different**

- California has among the strongest privacy laws in the United States, including:

  - **California Constitution** Article 1, § 1
  - **IPA California Information Practices Act** (Civil Code section 1798.17)
  - **CCPA California Consumer Privacy Act** §1798 *et seq.*
  - **CPRA California Privacy Rights Act** (eff. January 2023 replacing CCPA)
  - **CMIA California Medical Information Act** (Civil Code §56 *et seq.)*

Which of these, if any of these laws apply depends upon the nature of the breach and what information is hacked

California's ENS App

Will California state laws protect users from ENS data becoming a part of a fusion library of smartphone data…

Or….

Will U.S. PREP Act preempt ALL states privacy laws and provide immunity for ENS violations?

IMMUNITY FROM LIABIITY UNDER U.S. Public Readiness and Emergency Preparedness Act (PREP ACT)

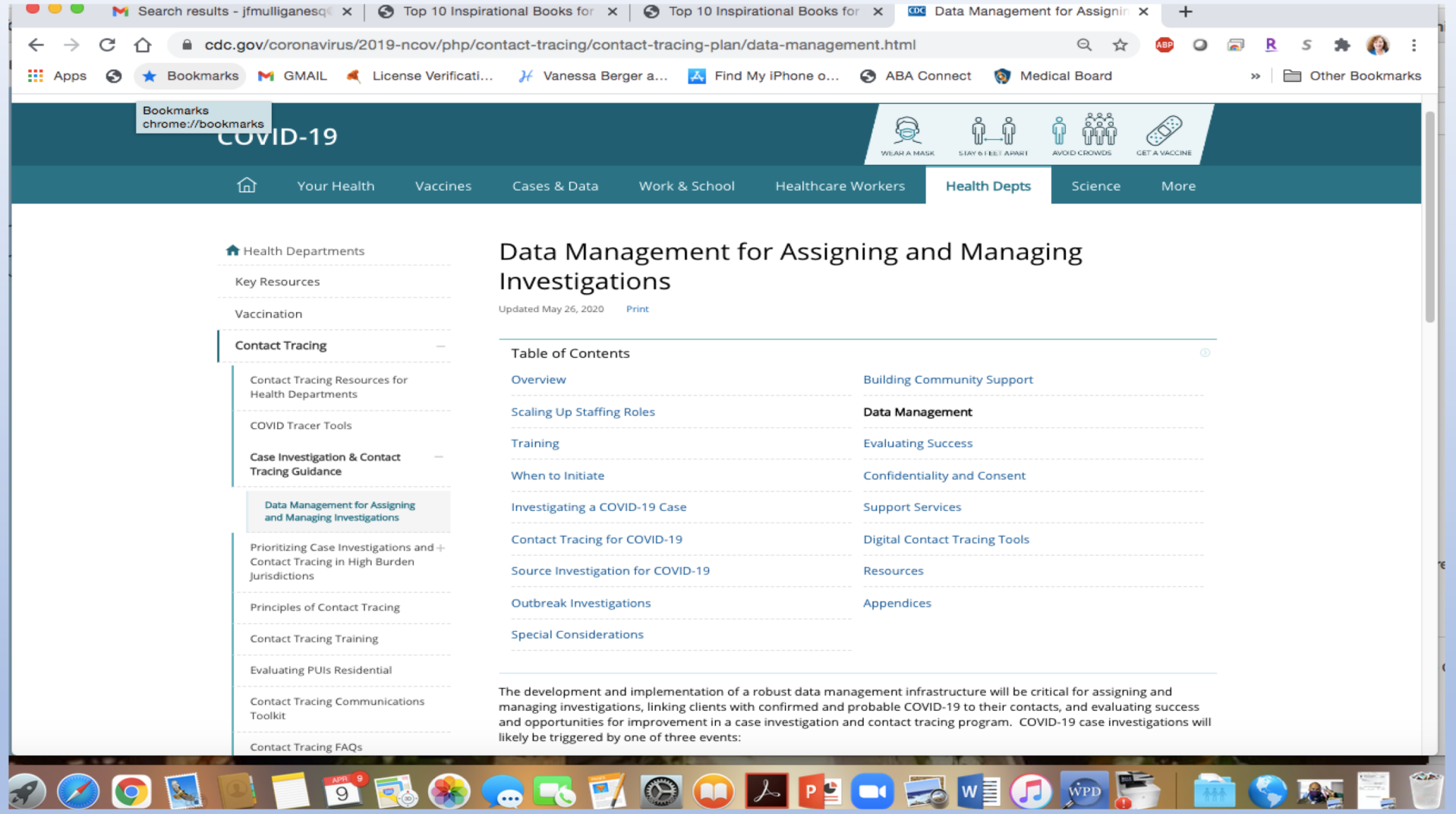
PREP Act is a federal statute enacted to encourage vaccinations, by granting broad waivers of liability for designated "countermeasures".

March 2020, The U.S. Department of Health and Human Services (HHS) made a COVID-19 public health emergency declaration, invoking PREP Act retroactively and ***continuing through October 1, 2024.*** **Countermeasures subject to immunity include:**

> " any …**device …used to prevent, or mitigate COVID–19 …**and all components …of any such product."

Later HHS Advisory Opinions qualified that for a pandemic product to have immunity it must also be either FDA approved or **described in an Emergency Use Instructions issued by the Centers for Disease Control (CDC).**

CDC emergency use instructions for ENS :



Will this trigger immunity under PREP Act for ENS privacy violations?

Federal PREP ACT immunity already preempts state laws in other areas traditionally regulated only by states

Example: Telehealth/Telemedicine

U.S. doctors' licensure is a question of state law, and all states *universally require* that doctors must be licensed in state where patient is located at the time the telehealth services are provided

In December 2020, the HHS extended the PREP Act to ***retroactively*** **grant immunity to such state licensing law violations related to the delivery of telehealth during the pandemic**

HHS Fourth Amendment to the Declaration Under the Public Readiness and Emergency Preparedness Act for Medical Countermeasures Against COVID–19 and Republication of the Declaration
December 2020 https://www.phe.gov/Preparedness/legal/prepact/Pages/4-PREP-Act.aspx

WILL THE PREP ACT IMMUNITY COVER MISUSE OF ENS DATA?

No ENS cases yet, but several cases are pending testing limits of PREP immunity to COVID countermeasures:

Estate of Maglioli v. Alliance HC Holdings New Jersey state court wrongful death case against a nursing home alleging negligence for failure to provide masks to employees or to screen for COVID.

PREP immunity defense asserted and defendant unsuccessfully attempted to remove to federal court. Trial court noted:

> "…many of the measures were ***not necessarily protected countermeasures*** such as "**social distancing, quarantining, lockdowns and others**. "

Case currently on appeal. Time will tell…..

What should be done to protect privacy with ENS data?

- Transparency about purpose of collecting information
- Define a retention period
- Create robust system for deleting data
- Safeguard data
- Restrict access to the data
- Create audit system for the data and process
- Devise robust statutory system of enforcement

COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes
Bradford *et al* Journal of Law and the Biosciences, 28 May 2020
https://academic.oup.com/jlb/article/7/1/lsaa034/5848138