Data Privacy & COVID-19 Response
WA Public Work Session

Kelsey Finch, Senior Counsel

July 28, 2020

FUTURE OF
PRIVACY
FORUM

Future of Privacy Forum

The Supporters

150+	25+	15+	5
Companies	Leading Academics	Advocates and Civil Society	Foundations

The Mission

Bridging the policymaker-industry-academic gap in privacy policy

Developing privacy protections, ethical norms, & responsible business practices

The Workstreams

- AI & Ethics
- Student Data
- Apps & Ad Tech
- Mobility & Location
- Privacy Enhancing Tech
- Smart Communities

1. Trends in Global Contact Tracing Apps
2. Emerging Best Practices
3. Hard Issues/Open Questions

Follow The Lead of Public Health Experts

- Data decisions should be driven by public health experts:
  - What data is collected?
  - How will it be used
  - How will the app be designed?
- Proximity tracking tools supplement, not replace, manual contact tracing
- Design and regulation must be flexible enough to adapt to evolving scientific evidence and the needs of public health authorities
- Ongoing monitoring of efficacy/effectiveness:
  - Judged against other interventions (e.g., mask wearing, social distancing, other technologies)

Global Trends: Contact Tracing & Exposure Notification Apps

Trends in the design of digital contact tracing tools:

- Decentralized vs. centralized
- Proximity (Bluetooth) vs. Location (GPS-based)
- Voluntary vs. Mandatory
- Processing official diagnoses vs. self-reported symptoms
- Non-app solutions: e.g., tracking bracelets, beacons, QR codes, self-reported symptoms

Voluntary vs. Mandatory

Consensus in Western democracies is that contact tracing apps must be **voluntary**.

- If individuals feel coerced into adoption, this could undermine trust in public health authorities and other strategies used to mitigate COVID-19
- Google-Apple Exposure Notification API only available for voluntary apps
- In a few global jurisdictions, contact tracing apps or tracking bracelets are mandatory (e.g., India, Turkey, Qatar, and Bahrain)

Centralized vs. Decentralized

Centralized

- Augments manual contact tracing
- Personal info collected by public health authorities
- Not based on the Google-Apple API

+ Alerts are accompanied by additional context for risk-based decision

+/- Broader range of public health purposes

- Risk of mission creep

Decentralized

- Parallel to manual contact tracing
- No personal info collected by public health authorities
- May or may not be based on the Google-Apple API

+ Lower privacy risks

- No additional context available about the proximity event

Location vs. Proximity

Precise Location Histories

- Apps rely on GPS and other signals (cell towers, WiFi) to generate precise location histories of devices
- Can be uploaded in real-time or shared voluntarily after diagnosis

+ Useful for aggregate trend analysis, identifying hot spots

- May not always be precise enough for exposure notifications, esp. urban/indoors

- Very challenging to de-identify

- Involves sensitive info (trust/adoption)

Proximity (e.g. Bluetooth)

- Devices emit ("chirp") random rotating identifiers ID's and store ID's "heard" by other devices
- Can be compared on-device against ID's of diagnosed people to trigger an "exposure notification"

+ If using the Google-Apple API, precise enough for under 6' exposures, and interoperable between devices

+ PHAs do not receive location data (more privacy-preserving, better trust/adoption)

- PHAs do not receive location data

	Centralized	Decentralized
Location History (GPS)	**_Box 1_** Israel (HaMagen) North Dakota (Care19) Rhode Island (Crush COVID RI) Utah (Healthy Together) Iceland (Rakning C-19)	**N/A**
Proximity (Bluetooth)	**_Box 2_** Australia (COVIDSafe app) France (StopCovid) Singapore (TraceTogether)	**_Box 3_** _*Google-Apple API_ CommonCircle Exposures (WA, _in develop’t)_ Germany (Corona Warn App) Switzerland (SwissCovid) United Kingdom _(in develop’t)_

Non-App Tracking Technologies

- **Tracking bracelets:** similar to apps, but could increase adoption for those without smartphones or who do not feel comfortable downloading an app; could reduce “false negatives” if worn consistently
- **Beacons:** Bluetooth beacons can be paired with phones to track location and send alerts, or send alerts when people stand too close
- **QR Codes:** businesses can choose to ask individuals to scan a unique QR code generated by an app, each time they enter or leave a building (*New Zealand*)

Public-Private Collaboration Beyond Digital Contact Tracing

Many other digital tools being developed commercially and used by PHAs - some share personal information with PHAs, some do not:

- Case management and identity resolution (Salesforce, others)
- Symptom surveys (Facebook - Carnegie Mellon)
- Research apps (UK's COVID Symptom Study app)
- Self-reporting and medical monitoring tools (SARA Alert System)
- Population trend analysis (Google's Community Mobility Reports)
- Chat bots for risk assessment, triage, and information (MS's Healthcare Bot)

Emerging Privacy Best Practices

- Be transparent about data collection and sharing
- Define appropriate purposes for data collection
- Define appropriate secondary purposes (if any)
- Specific retention limits
- Use privacy impact assessments

- Prioritize accessibility
- Be cautious of commercial SDKs (Software Development Kits)
- Avoid invasive or unnecessary permission requests
- Support interoperability
- Use security best practices (e.g., encryption, rotating Bluetooth identifiers)

Hard/Open Issues

- Are any secondary uses appropriate?
- Will tech tools exacerbate societal inequities?
- Will access to work, school, or other public spaces be based on app usage or health status?
- When should data collection and retention stop? When does the public health emergency end?
- How will essential public trust be maintained?

Thank you! Questions?

fpf.org, info@fpf.org, @k_finch, @futureofprivacy

surroundings.
Cell Towers
Nearby Wi-Fi Networks
Known Bluetooth Signals
CAFE
BANK
GYM
Proximity to Other Devices
HARDWARE
OS
APPLICATIONS
Shopping
Rideshare
Games
Weather
Social Media
Maps
2020-04-09 13:23:52
Lat 35.5/Lon 135.5
Allow "Weather" to access your location while you are using the app?
ALLOW WHILE USING
ALLOW ONCE
DON'T ALLOW
60% chance of rain!

layer for Apps to request access to a precise location measurement.

3 The **App** requests permission from the user via the OS.

4 The **OS** provides a precise location measurement and timestamp to the app.

More FPF Resources:

- Infographic: "Understanding the World of Geolocation Data"
- BrightHive & FPF "Responsible Data Use Playbook for Digital Contact Tracing"
- FPF Privacy and Pandemic Series, including:
  - Jules Polonetsky "Will I Install an Exposure Notification App? Thoughts on the Apple-Google API"
  - Gabriela Zanfir-Fortuna "European Union's Data-Based Policy Against the Pandemic, Explained"
  - FPF Wiki, COVID-19 Privacy & Data Protection Resources

Non-FPF Resources:

- John Hopkins University Press "Digital Contact Tracing for Pandemic Response"
- International Digital Accountability Council (IDAC): "An IDAC Investigation of COVID-19 Apps"

Processing Official Diagnoses vs. Self-Reported Symptoms

Self-reporting:

- Allowing self-reporting may increase the speed of notification, and help identify more community spreaders, reducing "false negatives" …
- … but could allow for security and integrity attacks

Official diagnoses*

- Only processing official diagnoses may decrease "false positives" …
- … but be too slow to control transmission, as COVID-19 can be transmitted before symptoms are apparent

**Google-Apple API only permits apps that rely on official diagnoses*

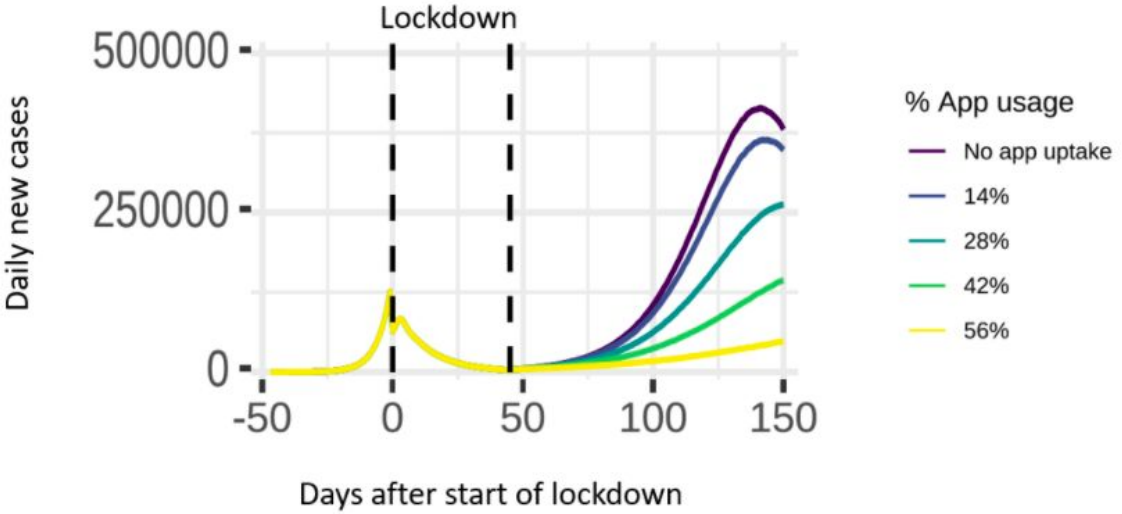
Effectiveness, utility & adoption rate

The 60% myth

Effectiveness factors:

- **User penetration**
- **Public trust**
- **Integration** and data sharing with other systems/apps
- Cross-border **interoperability** with other systems

If we reduce potentially infectious contacts by 20%, and 56% of the population use the app, we can considerably slow the epidemic. The app has an effect at all levels of uptake.


Lockdown
Daily new cases
Days after start of lockdown
% App usage
No app uptake