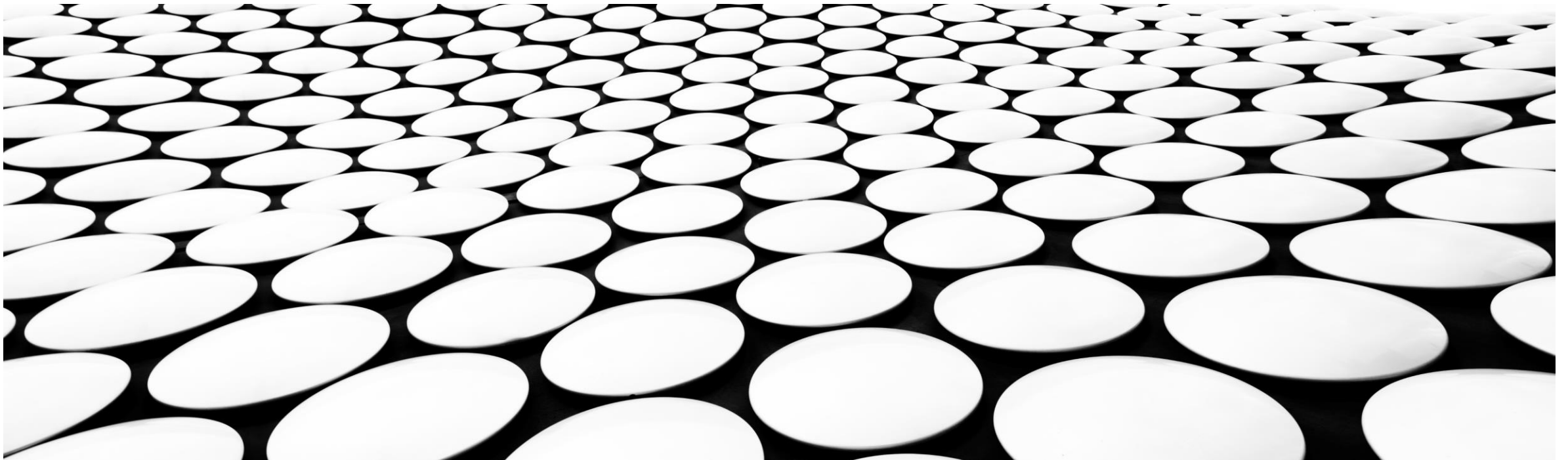

PRIVACY IN THE TIMES OF COVID-19 PANDEMIC

AMALIA BARTHEL, M.SC., PMP, CIPT, CDPSE, CIPM, CISM, CRISC

CRAIG BARRETTO, CISSP, GWAPT, OSCP



AGENDA

- Speaker Introduction
- Privacy and security concerns for the post lock-down world
- Why do we need to care
- Q&A

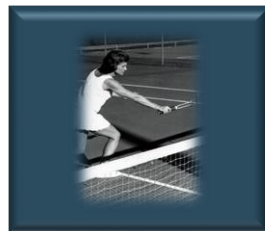
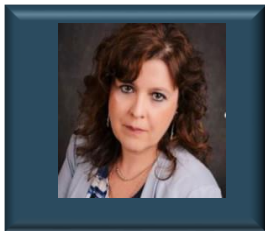


BIO – SPEAKER 1

AMALIA BARTHEL



AMALIA BIO



FOR THE MODERATOR

Amalia is a GRC & Privacy professional who has made it her mission to educate businesses about the importance of privacy for their corporate reputation and resilience.

Amalia works with Chief Privacy and Compliance Officers and CISOs in the health/Pharma, banking, telecom, the FinTech industry and Tech. /Cloud companies, retail, advertising/marketing, aerospace and public sector around the world, to advise on structuring the privacy program and alignment with internal GRC and Cyber Security efforts.

Amalia has authored/ co-authored many white papers and course material and is currently teaching business courses at University of Toronto, in the areas of IT Risk Management, Cybersecurity Risk Governance/Management and Privacy.

Amalia served on the Canadian IAPP Advisory Board, PMI (as Director on the Board of Directors of the Southern Ontario Chapter - SOC, now Toronto Chapter), and as an Advisor to the ISACA Toronto Chapter where she is actively managing a Mentoring program (as a volunteer) meant to help young professional enter the privacy profession.



BIO – SPEAKER 2

CRAIG BARRETTO



CRAIG BARRETTO





PRIVACY AND SECURITY CONCERNS FOR THE POST-LOCKDOWN WORLD

- DURING LOCKDOWN
 - POST LOCKDOWN
 - BASIC CONCEPTS AS
BUILDING BLOCKS
- 

THE WORLD IN LOCKDOWN

Personal

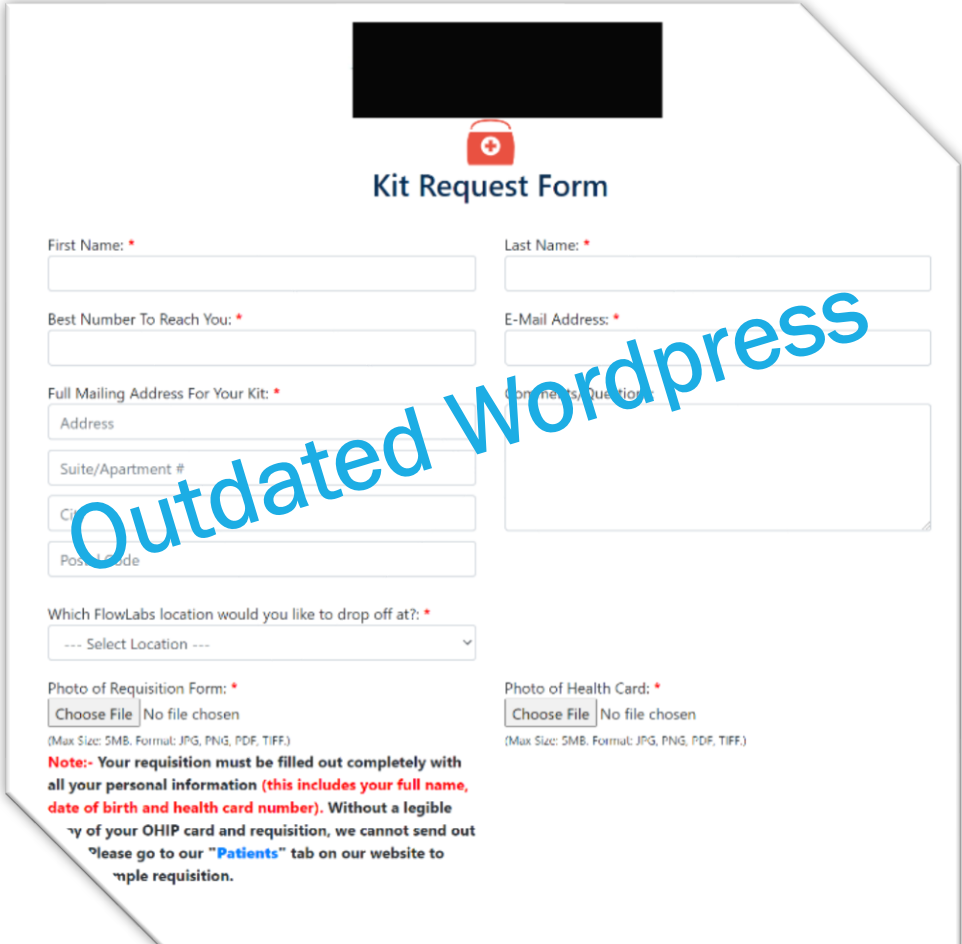
- Working from home using video-conferencing providers
- No contact with co-workers
- Some free tools for the people who lost their jobs (disgruntled employees)
- People ordering everything online (lots of personal information floating online)
- A lot more postings of a very personal nature via social media
- A lot of anxiety and mental health issues – people's use of recreational marijuana have increased


Enterprises

- Pandemic plans
- Heightened security attacks on organizations
- Busy HR – lots of people were let go (access termination???)
- Certain projects on hold / new priorities
- Massive rush to build e-commerce revenue (pressure to pump out code faster & lots more collection and processing of personal information)
- Some employers deployed tools to track the at-home online activity of employees (for “productivity” reasons)

NEW LOOK FOR HEALTHCARE PROVIDERS

- Online first – phone consults, video conferencing, reservations
- Identity verification (“send us a copy of your driver’s license”)
- Mistakes are being made




Kit Request Form

First Name: * Last Name: *

Best Number To Reach You: * E-Mail Address: *

Full Mailing Address For Your Kit: *

Address

Suite/Apartment #

City

Postal Code

Comments/Questions

Which FlowLabs location would you like to drop off at?: *
--- Select Location ---

Photo of Requisition Form: *
 No file chosen
(Max Size: 5MB, Format: JPG, PNG, PDF, TIFF)

Photo of Health Card: *
 No file chosen
(Max Size: 5MB, Format: JPG, PNG, PDF, TIFF)

Note:- Your requisition must be filled out completely with all your personal information (this includes your full name, date of birth and health card number). Without a legible copy of your OHIP card and requisition, we cannot send out your kit. Please go to our "Patients" tab on our website to complete requisition.

THE WORLD POST LOCK-DOWN – RELAXED MEASURES

Personal

- Some people are still working from home
- Some people are getting back to work or in newly opened stores – their temperature is taken which can lead to denied access
- Some people can't fully come back to work if they have to look after a relative affected by COVID-19 or an elderly parent who is isolated

Enterprises

- Governments have rules for getting back to work – like taking the temperature (where do those records go)
- Some knowledgeable privacy professionals are permanently eliminated (leaves a gap with IT, HR, Marketing ---→ risk!!!)
- Lots of mental health and anxiety issues

8 DIMENSIONS OF PRIVACY

- Privacy of person
- Privacy of thoughts, feelings and convictions
- Physical privacy (biometrics e.g fingerprints, facial recognition etc.)
- Privacy of behaviour and action
- Privacy of data and image (information)
- Privacy of communication
- Privacy of association
- Privacy of location and space (territorial)



WORLD HEALTH VS. PRIVACY – WHAT CAN GO WRONG

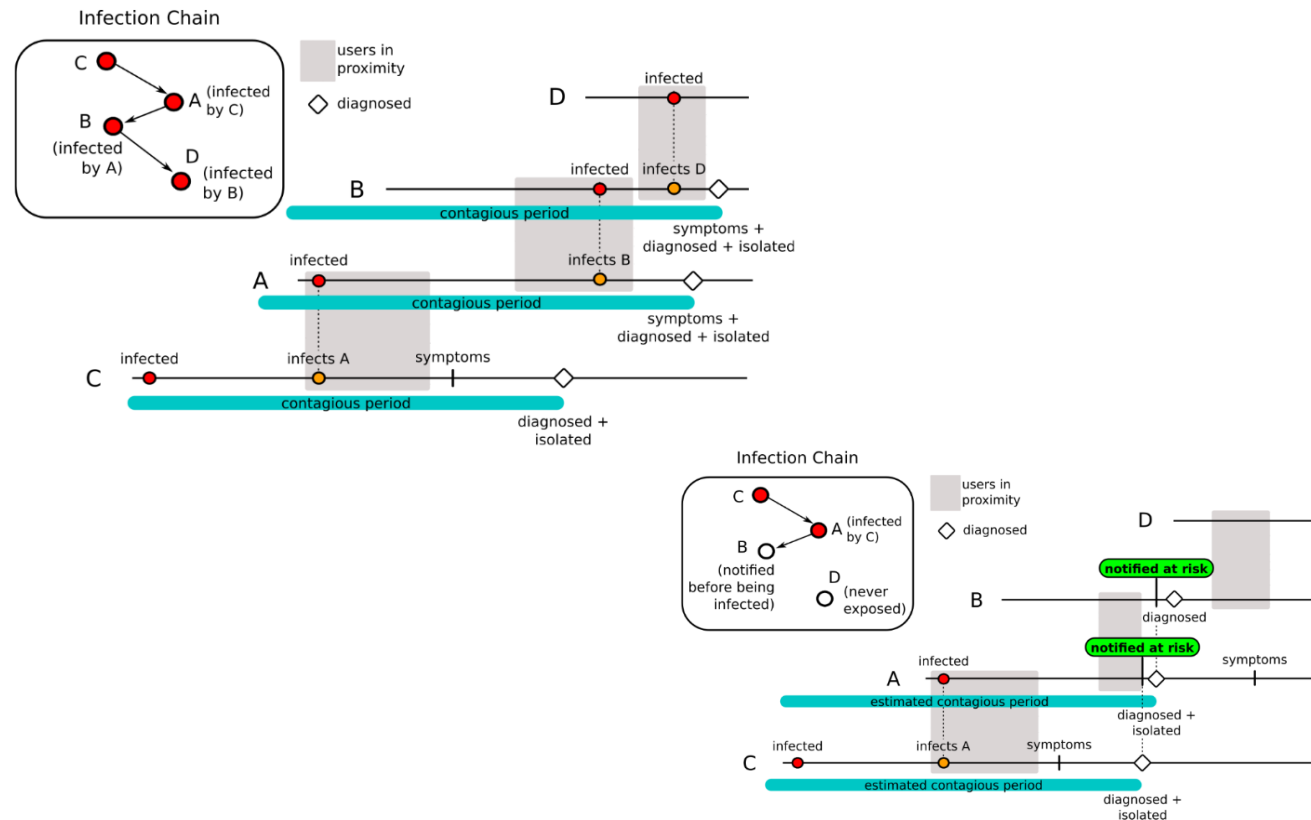
- Proposed contact-tracing apps
- Governments enforcing citizens tracking and surveillance
- Biometrics laws and enforcement

CONTACT-TRACING APP(MOBILE APP) – THE PROPER WAY

Guiding Principles

- Consenting participation (Open)
- Simple and Transparent
- Easy deployment – mobile app
- Anonymity – no personal data held
- Federated infrastructure – scaling worldwide

BENEFITS



Source: https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-specification-EN-v1_0.pdf

CONTACT-TRACING APP (MOBILE APP)

■ Privacy

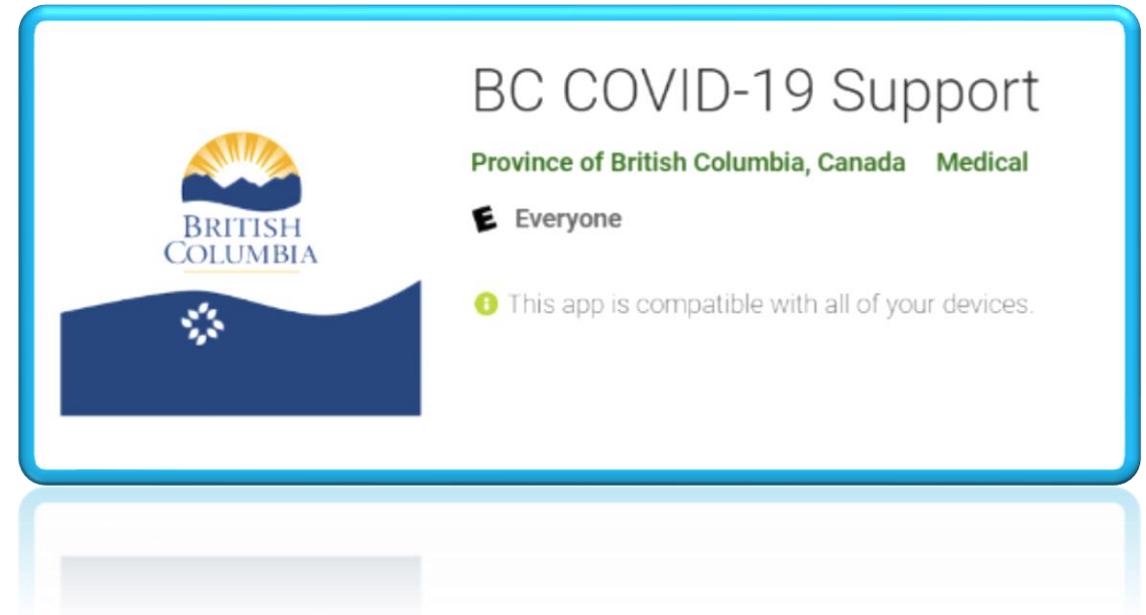
- Accuracy and Reliability of proximity data
- Anonymity of users from other users
- Anonymity of users from a central authority
- Assurance that there is no perceived Government surveillance and ultimately having this sensitive information in a massive government database
- Concern of what the Government may do with this data if in their hands given the global nature of the pandemic and different laws in different countries

■ Security & Architecture

- Risk of eavesdropping, injection of bogus messages or modification of messages
- Where data is stored & who can access it
- Ability to verify data – that it is reliable and correct
- Individuals identified as anonymous – their case gets a risk score and actions are being taken as a result (back-end servers) – identification based on Ephemeral Bluetooth Identifier
- Based on the risk score – the user’s “tracing information” is either deleted or a message is sent to their mobile App

TRACK ME IF YOU CAN

- Timely updates and important news
- Identify COVID-19 related symptoms
- Receive personalized recommendations



- Leaked residence GPS coordinates, postal codes, questionnaires and responses to a third party
- Loaded a default behavioural analytics SDK
- Looking to remove the tracking software altogether

DEMYSTIFYING THE BLUETOOTH TECHNOLOGY IN PBD MODE

- Bluetooth Low Energy – harder for governments to exploit the mobile phones for mass surveillance:
 - Who wants to perpetually leave their Bluetooth enabled (only to be traced everywhere)
 - OS of mobile phone apps have been designed to limit the exploitation of Bluetooth – but government agencies want backdoors
- Centralized systems: generally keep proximity data locally on the mobile phone until the person indicates that they are unwell and then the data is uploaded centrally – but who makes the decisions to inform the health authorities? (testing chaos)
- Decentralized systems: could also feed data centrally if you're required to enter data manually into the app, and presume that access to tests isn't a problem, so contact notifications are only sent out with a positive test result; and generally keep proximity data on devices both before and after diagnosis and receiving notifications (country wide-spread testing is being conducted)
- The core decision is about whether or not to notify others: centralised apps use some automated decision making to determine whether you're truly at risk and then decide whether to notify the people, or phones, you've interacted with. The decentralized apps require an actual test result before sending those notifications.

New exceptional rules:

- Limit by law and by design the number of purposes and uses for an app, eg an app we need to trust shouldn't be used for quarantine enforcement.
- Ask users to upload data sparingly and make it clear to them why each piece is important.
- Delete the data once this pandemic is over.
- Go further and delete the capability too: apps and APIs alike should be removed when this is done rather than try to find another purpose for them to exist.

COMING TOGETHER


- Exposure notification
- Limited to public health authorities
- No GPS tracking
- Identity masking



- June 18, 2020 – Canada announced plans to launch a contact tracing app.



WHY DO WE NEED TO CARE

- PRIVACY INVASIONS WITH POTENTIALLY IRREVERSIBLE CONSEQUENCES
 - DUTY OF CARE AND FIDUCIARY DUTIES IN THE LAW
- 

ACCOUNTABILITY

- Data breach lawsuits (including class actions)
 - *Tsige v. Jones*
 - Art. 82 GDPR – *Right to Compensation and Liability*
- Securities fraud class actions (misrepresentations on public statements)
- Directors' personal liabilities
 - Breach of fiduciary duties and other torts
 - Statutory (*Quebec - Act respecting the protection of personal information in the private sector*)
- Shareholders derivative lawsuits
- Breach of contractual obligations
- Breach of legislations with penal dispositions (e.g. GDPR)
- Potential for more lawsuits derived from Pandemic-adverse actions of employers towards their staff
- Competition Bureau of Canada enforcement powers (see Facebook fine – 9 mil. In May 2020)



PRIVACY IN HEALTHCARE

- Will you be asked if you have a contact-tracing App and should you update it if you become infected
- How will false alarms be prevented? Who updates the App? (Governing the response in the Contact-tracing app)
- Where is the temperature data going? Who has it? For how long?

TAKING THE TEMPERATURE IN AIRPORTS

- Forbidden in Netherlands (by Dutch Data Protection Law)
- Heathrow and Ch de Gaulle (France) airports have designated zones of screening (not sure how private that is)
- Prague airport in the Czech Republic has designated separate gates for all passengers arriving from Italy. Airport employees have been directed to closely monitor passengers arriving from Italy and report any signs of respiratory disease to airport security. Frequent disinfection of arrival gates, buses and other areas handling passengers from Italy are also planned.
- Bratislava airport in Slovakia has implemented strict screening measures for passengers arriving from Italy, who are required to fill out a questionnaire to enable officials to identify any suspected cases.
- Canadian airports including Toronto international airport, Montreal international airport, and Vancouver international airport have announced that international passengers will have to undergo additional screening such as temperature and other symptomatic checks and inquiring about their visits to Wuhan to check for the possibility of having contracted the infection.
- Is this a temporary measure? (what is temporary?) From what destinations?
- Crew additional protective gear on the plane? If asymptomatic passengersfor how long?
- What about security checkpoints? One has to ask about hand sanitizers (is it still allowed in small quantities?)

TAKING THE TEMPERATURE IN THE WORKPLACE

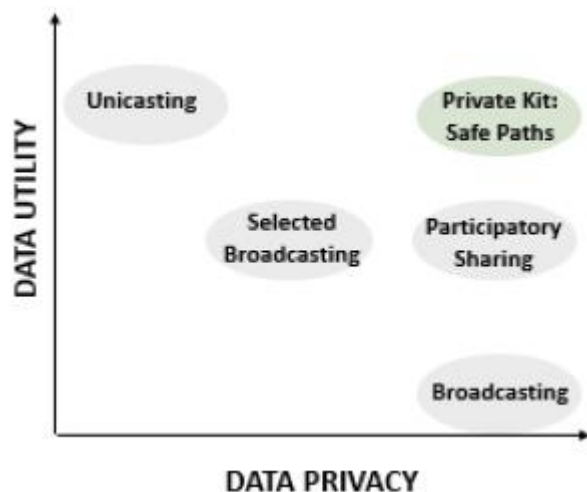
- No indicator someone has COVID-19 – can lead to discrimination/ stigma / blame / negative reaction of co-workers
- Needs to be done in private with a Sr. HR staff present and medical personnel
- In the US – these checks are NOT subject to legislation (HIPAA) & in Canada – same – there are no such protections, given that regular business organizations are not subject to Health Legislation
- Employers: think carefully about whether and how to record the information (do not include it in personnel files).
- Employees: know your rights – you can't be discriminated against! (especially where there is no conclusive evidence)

BIOMETRICS OR THE CURIOUS CASE OF BENJAMIN BUTTON

- Unprepared (some old) laws : is face recognition now associated with temperature???
- Illinois Biometric Privacy Act. It primarily covers issues relating to biometric data which can be used in conjunction with potential identity theft including “access [to] finances or other sensitive information.” Illinois, which regulates the collection, use, and destruction of biometric identifiers typically limits what it considers in this category as “a retina or iris scan, fingerprint, voiceprint or scan of hand or face geometry,”
- specifically states that biometric identifiers do not include signatures, human biological samples used for valid scientific testing or screening, and similar items.
- Should people’s “body temperature” be considered as another personal identifier?
- Currently such an identifier may be used in a discriminatory manner (denied access on the plane for example)
- What about the Right-to-be-Forgotten / Right to Erasure?
- PIPEDA allows organizations to collect, use or disclose information only for purposes that a reasonable person would consider appropriate in the circumstances (subsection 5(3)). However there is an exception: *“If the use or disclosure is for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual (paragraphs 7(2)(b) and 7(3)(e)), such as if an individual requires urgent medical attention, and they are unable to communicate directly with medical professionals.”*

Table 1: The various contact-tracing technological approaches are mapped against the reviewed risks and challenges.

FOR THE DEVELOPER ENTHUSIASTS



Technological Intervention	Broadcast	Selected Broadcast	Unicast	Participatory	PrivateKit: Safe Paths Phase 1 (Broadcast)
ACCURACY	Limited	Limited	High	Limited	High
ADOPTION	High	Medium	Medium	Low	Medium
1. Privacy					
Privacy risks for carriers	Significant	Moderate	Moderate	Significant	Moderate to Low, although only redacted location trails are released to the public, a small chance for public identification remains.
Privacy risks for local businesses	Significant	Significant	Moderate	Significant	Moderate to Low, although only redacted location trails are released to the public, a small chance for public identification remains.
Privacy risk for users	Privacy protected	Privacy at risk	No privacy	Privacy protected	Privacy protected
Privacy risk for non-users	Privacy at risk if carriers are identified	Privacy at risk if carriers are identified	Privacy at risk if carriers are identified	Privacy at risk if carriers are identified	Privacy at risk if carriers are identified
2. Consent					
Consent of carriers	Practices vary	Practices vary	Practices vary with limited or no consent most frequently applied	Full consent	Full consent
Consent of businesses	Rare	Rare	Rare	Unlikely	Depends on government practice
Consent of users	Not applicable	Consent mostly needed	Consent mostly needed. Consent to make public their information once their are a carrier is typically required to become a user.	Not applicable	Consent needed
3. Systemic challenges					
Misinformation and panic	High risk	Medium risk	Medium risk	High risk	Medium risk
Panic	High risk	High risk	Low risk	High risk	Low risk
Risky behavior	Low risk	Low to medium risk	High risk, especially if the system is widely used	Low risk	Medium risk, due to a strong, user focused educational campaign
Fraud and abuse	High risk	High risk	High risk	High risk	Low risk, the identity of carriers and businesses are not publicized and access to the system is controlled
Security of information	Low to medium risk	Low to medium risk	High risk, large data collection appeals to bad actors	Low risk, carriers choose to share their information publicly	Low to medium risk, user data is not collected and carrier location trails are distributed among local government entities
Equal access	Mostly accessible	Limited by technological requirements (smartphone, battery, certain OS asf.)	Limited by technological requirements (smartphone, battery, certain OS asf.)	Limited by technological requirements (smartphone, battery, certain OS asf.)	Limited by technological requirements (smartphone, battery, certain OS asf.)
Socioeconomic factors	Low-income earners unequally affected	Low-income earners unequally affected	Low-income earners unequally affected	Low-income earners unequally affected	Low-income earners unequally affected

Q&A



Kylie Jenner ✓

@ikyliejenner

Can you guys please recommend books that made you cry?



Saransh Garg @saranshgarg

Replying to @ikyliejenner

Data Structures and Algorithms in Java (2nd Edition) 2nd E

by Robert Leflore (Author)

★★★★☆ 114 customer reviews

[Look inside](#)



Kindle \$29.80

Hardcover
\$33.89 - \$45.04



Paperback
\$23.39 - \$27.18

☐ Buy used

☒ Buy new

In Stock

THANK YOU

-  amalia.c.barthel@gmail.com
-  barrettocraig@gmail.com
- <https://sites.google.com/fpf.org/covid-19-privacy-resources>