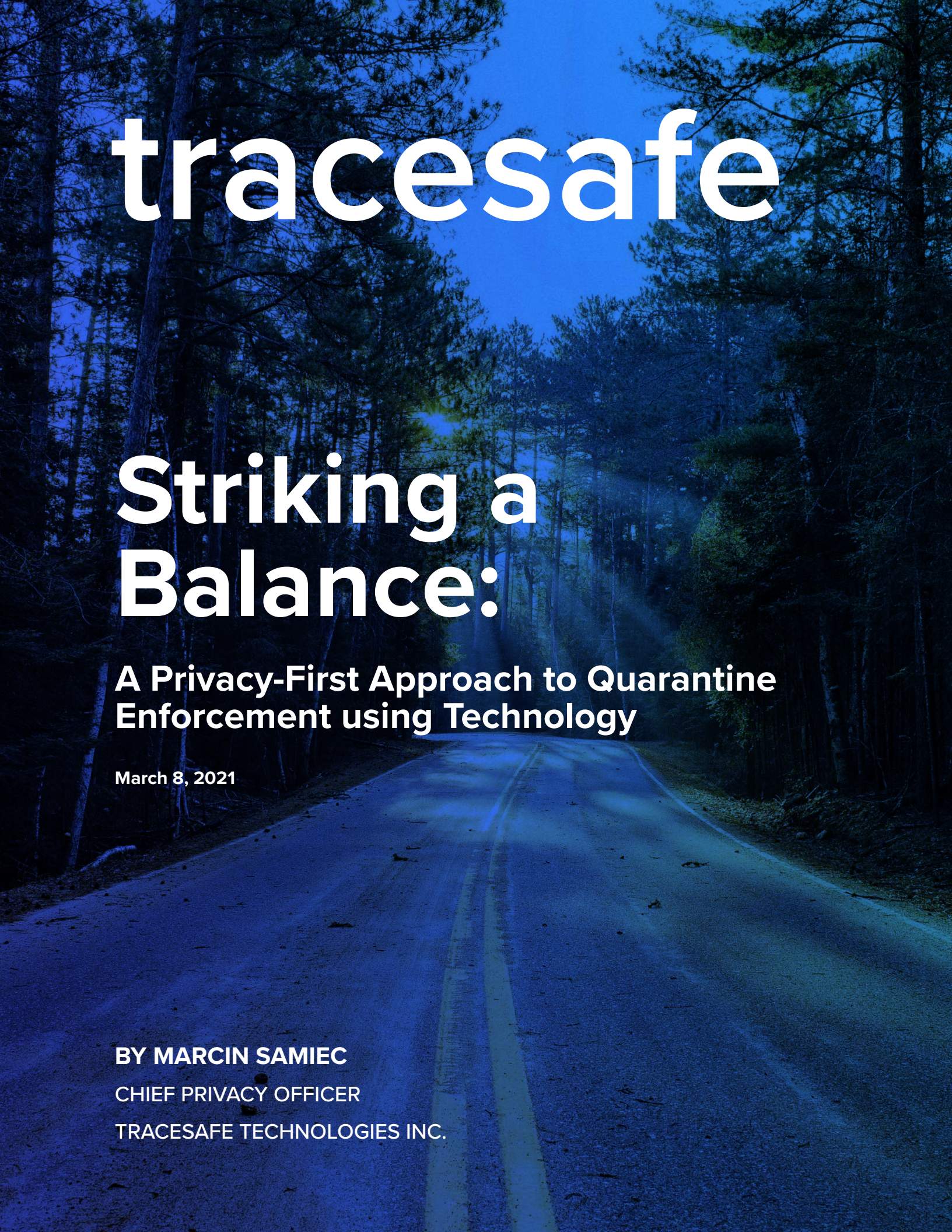


tracesafe

Striking a Balance:

A Privacy-First Approach to Quarantine Enforcement using Technology

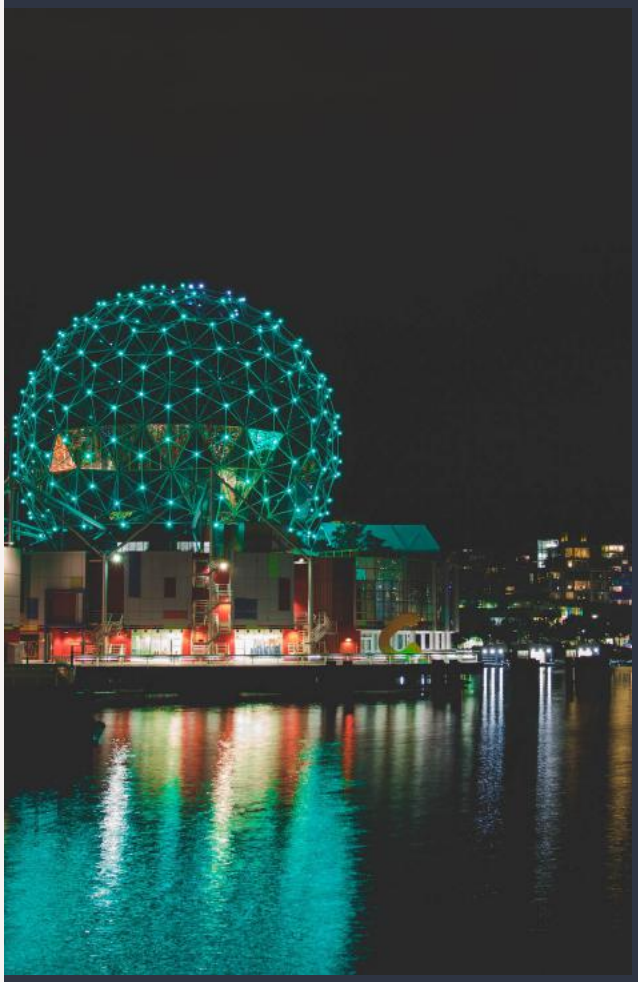
March 8, 2021

BY MARCIN SAMIEC

CHIEF PRIVACY OFFICER

TRACESAFE TECHNOLOGIES INC.

CONTENT



SECTION 1

INTRODUCTION

Quarantine enforcement has long been an effective tool for countries to manage the spread of COVID-19, and technology has been used in different ways by countries to aid in its effectiveness.

In a worldwide pandemic, there's a tightrope that needs to be walked between privacy and public health. It's the balance that is struck every time the public is asked to wear masks, or when incoming international travellers are required to quarantine. If the public fails to temporarily limit their movements and change their behaviours, it can ultimately result in the proliferation of a deadly disease and its variants.

Quarantine enforcement has long been an effective tool for countries to manage the spread of COVID-19, and technology has been used in different ways by countries to aid in its effectiveness. But with the use of technology in privacy-sensitive areas like quarantine enforcement, there is an important discussion to be had about civil liberties and the purported invasion of privacy that can result.

For too long, rights-focused countries like Canada have grappled with the false dichotomy of privacy vs. civil liberties, where one concept must win entirely at the expense of the other. This false dichotomy exists even though human rights legislation worldwide is predicated on the notion of balance between rights.

Fortunately, a Canadian-born framework called Privacy by Design ensures that if a technology is built on its seven principles, it can respect user privacy without sacrificing essential technical features.

This white paper explores the use of technology in quarantine enforcement, the resulting privacy and civil liberty issues, and argues that when technologies are built on strong privacy principles, they can effectively strike a balance between privacy and public health and help governments build trust with their citizens.

This white paper also features TraceSafe, a privacy-first company with roots in infant tracking that has developed a solution for privacy-conscious governments and organizations around the world who require an effective technological aid in preventing the spread of COVID-19.

Quarantines Are Effective, When Enforced

In September 2020, the World Health Organization commissioned a Cochrane Rapid Review[1] to assess whether and how effectively quarantine stops COVID-19 from spreading. The review found that quarantines work; those countries that have implemented strict quarantine measures, including Australia, New Zealand, Singapore, Taiwan and Vietnam, have almost completely eradicated the virus with seven-day averages of less than 10 cases.[2]

The review included 51 studies and found that "early implementation of quarantine and combining quarantine with other public health measures" was important and effective in combating the spread of COVID-19. Quarantine alone was found to reduce the spread of infection by 44-96%, the number of deaths by 31-76%, and viral reproduction by 37-88%.

Countries have taken different approaches to quarantine enforcement. They range from using little to no technology and relying on government officials and security firms to check for compliance (as is the case in Canada), to the use of wearables, facial recognition-equipped cameras, and drones. Each of these approaches presents the need to balance the privacy of the individual under quarantine against public health interests.

"Quarantine alone was found to reduce the spread of infection by 44-96%"

1. Barbara Nussbaumer-Streit et. al. (2020) Quarantine alone or in combination with other public health measures to control COVID-19: a rapid review *https://www.cochranelibrary.com/cdsr/doi/10.1002/14651858.CD013574.pub2/full*

2. At the time of writing, the seven-day average for Australia, New Zealand, Singapore, Taiwan and Vietnam are as follows: 7, 3, 10, 2, and 9 as per Google Statistics when searching "covid cases [country]"

SECTION 2

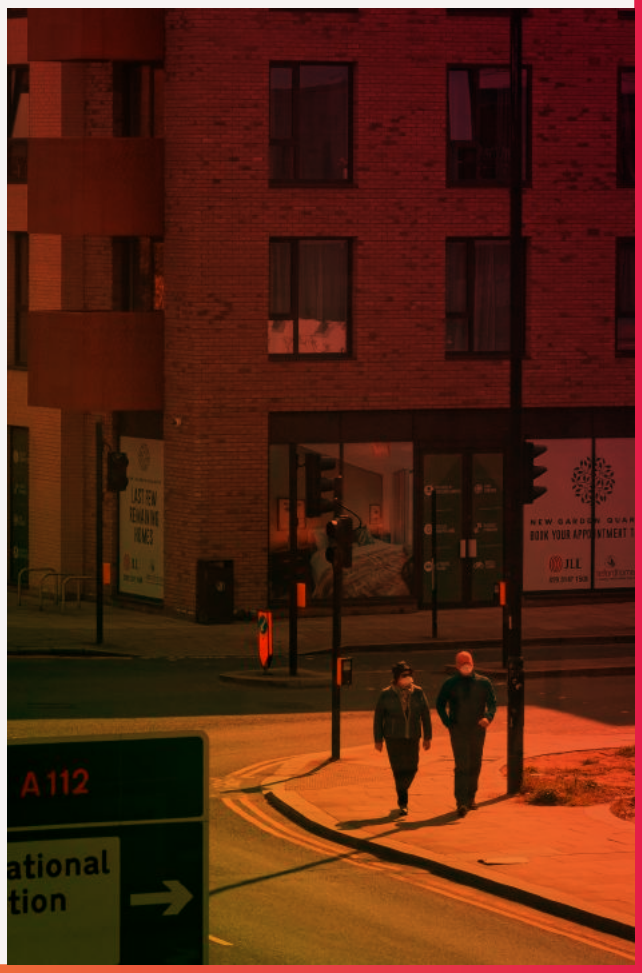
TECHNOLOGY USE
IN QUARANTINE ENFORCEMENT

In Governing Covid-19 through Digital Technologies: A Global Perspective,[3] Aghaei, Guo, and Sulaiman provide an overview of the technologies used across nine countries, including Switzerland, Singapore, Germany, the UK, South Korea, Israel, Taiwan, Russia, and China/Hong Kong, and note:

"When a person tests positive for Covid-19, there is an almost universal consensus that they ought to be temporarily quarantined from the rest of the public, in order to both protect the rights of uninfected persons and limit the danger to the public health generally.

While it is theoretically possible to accomplish quarantine enforcement without the use of digital technology, the staggering rates of infection around the world suggest that this is not a feasible tactic for even those nations with robust law enforcement."

Quarantine enforcement without digital technology [...] is not a feasible tactic.



3. Armin Aghei (2020) Governing COVID-19 through digital technologies: A Global Perspective https://cyber.harvard.edu/sites/default/files/2020-07/GDT%20COVID%20FINAL%20PAPER.pdf

SECTION 3

Privacy and Civil Liberty Issues

The use of technology for quarantine enforcement is often a point of contention for countries that are individual rights-focused. These countries have, in some cases, tried to limit the use of technology in an attempt to safeguard individual liberties. However, by erring too far on the side of caution, and without balancing community health and safety, this tactic may result in an ineffective approach overall.

In Canada, Section 8 of the Canadian Charter of Rights and Freedoms[4] guarantees that everyone has the "right to be secure against unreasonable search or seizure." But it is well understood that privacy rights are not absolute and must be balanced with the interests of public health and safety.[5] This is explicit in the limitation clause of Section 1 of the Charter.

This notion of balance is present in human rights legislation around the world, including the Universal Declaration of Human Rights (1948), European Convention on Human Rights (1950), and Charter of Fundamental Rights (2000).

Rights-focused countries like Australia and New Zealand have recognized this balance, implementing strict quarantine measures and temporarily restricting civil liberties in the attempt to contain the virus and return life back to normal. Both countries, at the time of writing, have a seven-day average of 7 and 3 COVID-19 cases respectively and have largely resumed "normal" daily activities.[6]

It is well understood that privacy rights are not absolute and must be balanced with the interests of public health and safety.

5. A principle also known as a proportionality analysis. See, e.g. Canada (Attorney General) v. JTI-Macdonald Corp., [2007] 2 S.C.R. 610, at paragraph 36.

6. Solarina Ho (2020) Yes, millions of people are living a relatively normal, coronavirus-free life https://www.ctvnews.ca/health/coronavirus/yes-millions-of-people-are-living-a-relatively-normal-coronavirus-free-life-1.5249917

EXPLORING THE FALSE DICHOTOMY

PRIVACY VS. CIVIL LIBERTIES

In Canada, the seven-day case count average is 2,839. Unlike Australia and New Zealand, the focus in Canada has too long been on the false dichotomy of privacy vs. civil liberties and a commonly held belief that technology is inherently privacy-invasive.

As a result, Canada has employed a traditional approach to quarantine enforcement. It recently imposed mandatory three-day hotel stays for incoming travellers with hefty out-of-pocket expenses (approximately $2,000 per person) before asking travellers to continue their quarantine at home. This solution is costly both for incoming travellers and the government, yields little data for the government to analyze the effectiveness of the program, and is burdensome to maintain.

Technology is an important tool for quarantine enforcement, but a delicate privacy balance needs to be struck.

Technology is an important tool for quarantine enforcement, but a delicate privacy balance needs to be struck. On one end of the spectrum, not using technology at all is old-fashioned, costly, and impedes effectiveness. On the other end of the spectrum, as in China and Russia with preexisting surveillance frameworks, technology can certainly go too far. In those cases, it can lead to fears of an Orwellian state control that puts civil liberties at risk.

There are effective ways to balance privacy and public health. One way to strike that balance is by implementing technologies that are built on the Privacy by Design framework[7] and align with the Personal Information Protection and Electronic Documents Act (PIPEDA)'s 10 fair information principles,[8] both of which were developed in Canada. At TraceSafe, this is called the "Privacy-First" approach.

There are effective ways to balance privacy and public health... at TraceSafe, this is called the "Privacy-First" approach.

7. Ann Cavoukian (2011) Privacy by Design The 7 Foundational Principles https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

8. The Personal Information Protection and Electronic Documents Act is a Canadian law relating to data privacy. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

SECTION 4

A PRIVACY-FIRST APPROACH

Technologies lie on a spectrum between "privacy-invasive" and "privacy-first," depending on their intent and the philosophies that underpin them. Privacy-first technologies are principles-led and seek to maximize outcomes for both parties, whereas privacy-invasive technologies tilt the scale of benefits in favour of the owner of the technology at the expense of the user.

Privacy by Design[9] is a framework originally developed by the former Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian. It includes seven principles for ensuring that new technologies are built with privacy as the top priority. Privacy by Design is a Canadian-born and internationally recognized approach encoded into Europe's General Data Protection Regulation (GDPR) as Article 25.[10]

If a solution has been built on the Privacy by Design framework, it means it was designed with privacy as its top priority, integrated by default. It eliminates the outdated, zero-sum approach where either technology supersedes privacy or vice-versa. With Privacy by Design, user privacy can be maintained without sacrificing any essential technical features.

Another way to create a privacy-first technology is to build it on **PIPEDA's 10 fair information principles**. These principles form the ground rules for the collection, use, and disclosure of personal information.

TraceSafe has created a privacy-first solution for governments and organizations that not only respects user privacy but has been used effectively for quarantine enforcement around the world.

If a solution has been built on the Privacy by Design framework, it means it was designed with privacy as its top priority, integrated by default.

9. Ann Cavoukian (2011) Privacy by Design The 7 Foundational Principles https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

10. Article 25 EU GDPR "Data protection by design and by default" https://www.privacy-regulation.eu/en/article-25-data-protection-by-design-and-by-default-GDPR.htm

SECTION 5

A PRIVACY-FIRST SOLUTION

iMSafe

TraceSafe's technology was originally developed to track newborn infants in real-time in New Zealand. It has since evolved to provide world-leading quarantine management solutions to governments around the world, including in Hong Kong, Singapore, and the Cayman Islands.

This technology, called "iMSafe," was also used to manage the tournament quarantine bubble at the 2021 World Junior Hockey Championship in Edmonton, Alberta.

The iMSafe solution is intuitive. It's made up of a sleek, disposable wristband and a centralized admin dashboard.

When deployed at airports, it follows a simple four-step process:

1. A traveller receives a wearable. A clerk scans the QR code and registers the traveller using pseudonymized information.
2. The traveller downloads an app and scans the QR code on their wearable.
3. The traveller uses the app to check in once they reach their designated quarantine location.
4. Periodic presence checks are made with the traveller's acknowledgement. Alerts are generated if there is no re-sponse, the tag is unreachable from the phone, or if the tag has been tampered with.

In 2020, that same technology used to track arguably the most precious assets – infants – was quickly and seamlessly adapted to the quarantine needs of governments around the world.

TECHNOLOGY FOR INFANT SAFETY

In 2016, hospital managers of the maternity wards in Counties Manukau District in New Zealand were looking for a reliable infant tracking solution after a slate of troubling infant abduction cases.

The CEO of TraceSafe Technologies, Dr. Dennis Kwan, worked with the maternity team to develop unob-trusive wristbands and a technology infrastructure to track newborns. Doctors and hospital staff could check a dashboard to see, in real-time, where an infant was on the ward. Trespasses outside the confines of the maternity wards would trigger instant alerts to nursing staff. Tampering or removing the wristband would also trigger alerts.

In 2020, that same technology used to track arguably the most precious assets - infants - was quickly and seamlessly adapted to the quarant-ine needs of governments around the world.

A

APPS NOT MANDATORY: GATEWAYS ADD PRIVACY OPTIONS

In cases where travellers are unable or unwilling to use their smartphones, iMSafe provides another privacy-honouring option for end users. In July 6, 2020, TraceSafe announced the introduction of the iMSafe Gateway, a GPS and LTE-enabled device that replaces the need to pair a user's smartphone with the wristband.

This small box, no larger than an Apple TV, enhances privacy protection by eliminating the need for a smartphone altogether and streamlines the user experience, providing a clean end-to-end solution.

B

MINIMAL DATA COLLECTION

Minimal Data Collection
In accordance with Principle 4 of PIPEDA's 10 fair information principles, TraceSafe only collects the minimum amount of information necessary to ensure quarantine management. When used with the smartphone option, the information collected includes:

- A traveller's name or a unique, pseudonymous identifier (the latter is more privacy-preserving).
- The location (latitude and longitude) of where the traveller is expected to quarantine (for example, a hotel).
- The location (latitude and longitude) at regular intervals of time to check if the traveller is quarantining during his/her quarantine period.
- The traveller's confirmation through the iMSafe application that they are at their designated quarantine location.

No other information from a user's device is collected.

When used with the gateway option, the information collected includes:

- A traveller's name or a unique, pseudonymous identifier (the latter is more privacy-preserving).
- The traveller's proximity to the iMSafe Gateway device at regular intervals of time to check if they are in their designated quarantine location.

PRIVACY BY DESIGN PRINCIPLE	HOW IMSAFE COMPLIES
1. Proactive not Reactive; Preventative not Remedial	• Chief Privacy Officer (CPO) involved in product development • Robust privacy program in place • Data Protection Impact Assessment process in place • CPO partners with third-party privacy consultants to audit the privacy program
2. Privacy as the Default Setting	• Gateway option for added privacy • Minimal data collection • Disposable wristbands only have a 20-30 day battery life
3. Privacy Embedded into Design	• Ability to pseudonymize data to prevent storing full names • Minimal data collection
4. Full Functionality — Positive-Sum, not Zero-Sum	• Full featured solution with minimal data collection and end-to-end security
5. End-to-End Security — Full Lifecycle Protection	• Ability to automatically delete data after a specific number of days • Solution can be hosted on government/ organization cloud account, in a local geographic area • Wearables secured against replay attacks, tampering, and are encrypted with RC5 encryption • All HTTPS and communication is done over a secure 1.2 TLS channel
6. Visibility and Transparency — Keep it Open	• Third-party privacy consultants audit the privacy program • Detailed Privacy & Cookie Notice • Partnered with EU and UK Representatives (GDPR, Article 27) • Data Subject Request Procedure
7. Respect for User Privacy — Keep it User-Centric	• Simple user interface • Detailed Privacy & Cookie Notice • Minimal data collection

MOBILE APPLICATION

A custom mobile application is used both by administrators to onboard travellers and by travellers when they choose to use their smartphones to configure iMSafe. For administrators, it facilitates easy setup and traveller registration.

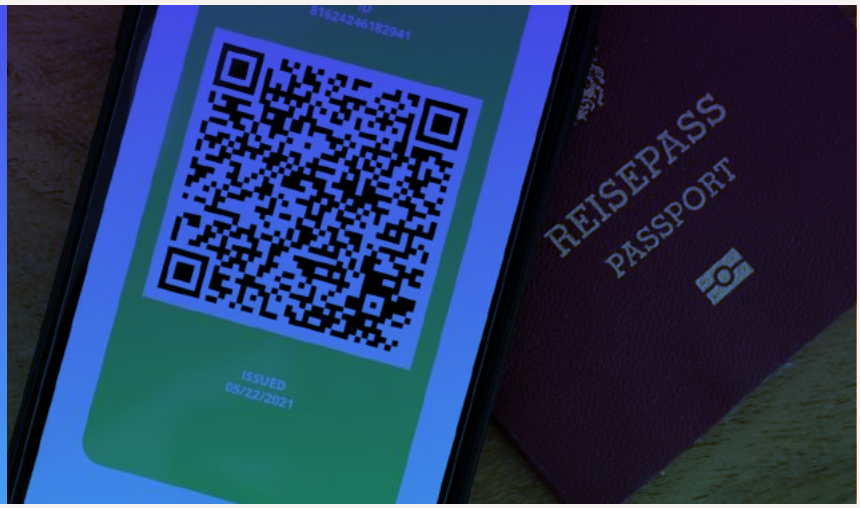
For travellers, it provides an easy-to-use interface that allows them to respond to alerts if they go beyond the physical limits of their quarantine location, or tamper with their wristbands.

ADMIN DASHBOARD

An intuitive web interface provides administrators with detailed reports of user quarantine status, user history with location details, and actionable alerts.

The dashboard provides information such as:

- A pseudonymized count of active users, users who have completed a quarantine period, and the number of users onboarded by the administrator
- A count of active users for whom alerts have been generated. For example, a person away from their phone (phone unreachable), a person not reaching their quarantine location, a person leaving their quarantine location, etc.



Mobile apps are hosted in the application stores of government or healthcare authorities.

SERVER AND MOBILE APP HOSTING

TraceSafe offers flexible deployment options, including the ability to deploy on the public cloud (AWS), private cloud, or on-premise servers. It is strongly recommended to host the application in a cloud or server instance owned or referred by the government, allowing authorities to focus on the health and safety of Canadians.

For cloud deployments, TraceSafe uses Amazon Web Services (AWS) as the vendor of choice. AWS is ISO/IEC 27001:2013, 27017:2015, and 27018:2019 certified, and allows us to securely host data in geographical areas that correspond to our client's needs based on relevant privacy laws (ie. hosted in Canada).

Mobile apps are hosted in the application stores of government or healthcare authorities, complying with the rules set by Apple and Google for COVID-related applications.

TraceSafe provides rebranding, hosting assistance and app maintenance, allowing authorities to focus on the health and safety of Canadians.

SERVER AND MOBILE APP HOSTING

iMSafe, with its well-defined APIs and SDKs, can seamlessly integrate with other applications, including contact tracing applications, health monitoring applications, existing COVID management applications, and customized web dashboards.

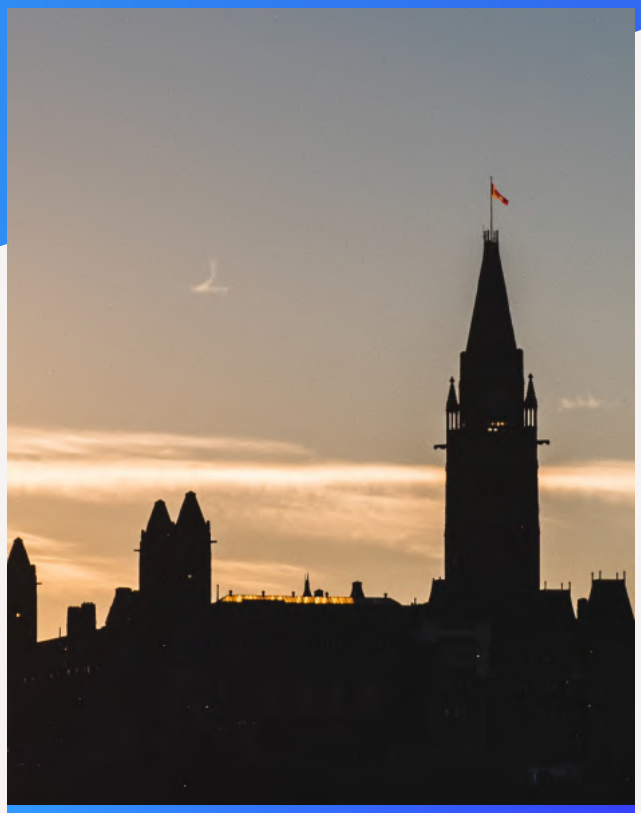
SECTION6

How iMSafe Builds Trust between Government and Citizens

Public trust is an essential component of good governance, especially during times of uncertainty and crisis.[11] When a government shows the capacity, expertise and technical knowledge to make decisions in the public's best interest, trust increases. In turn, the government is more enabled to respond effectively to the COVID-19 pandemic.

When expert technology solutions are deployed in the interest of public health and safety, in a transparent and privacy-first framework, feedback from the public is overwhelmingly positive.[12] Travellers are aware that the privilege of international travel comes with some responsibilities to their fellow citizens, namely quarantining. It is the job of the government to make quarantining as seamless as possible in order to increase compliance and public confidence.

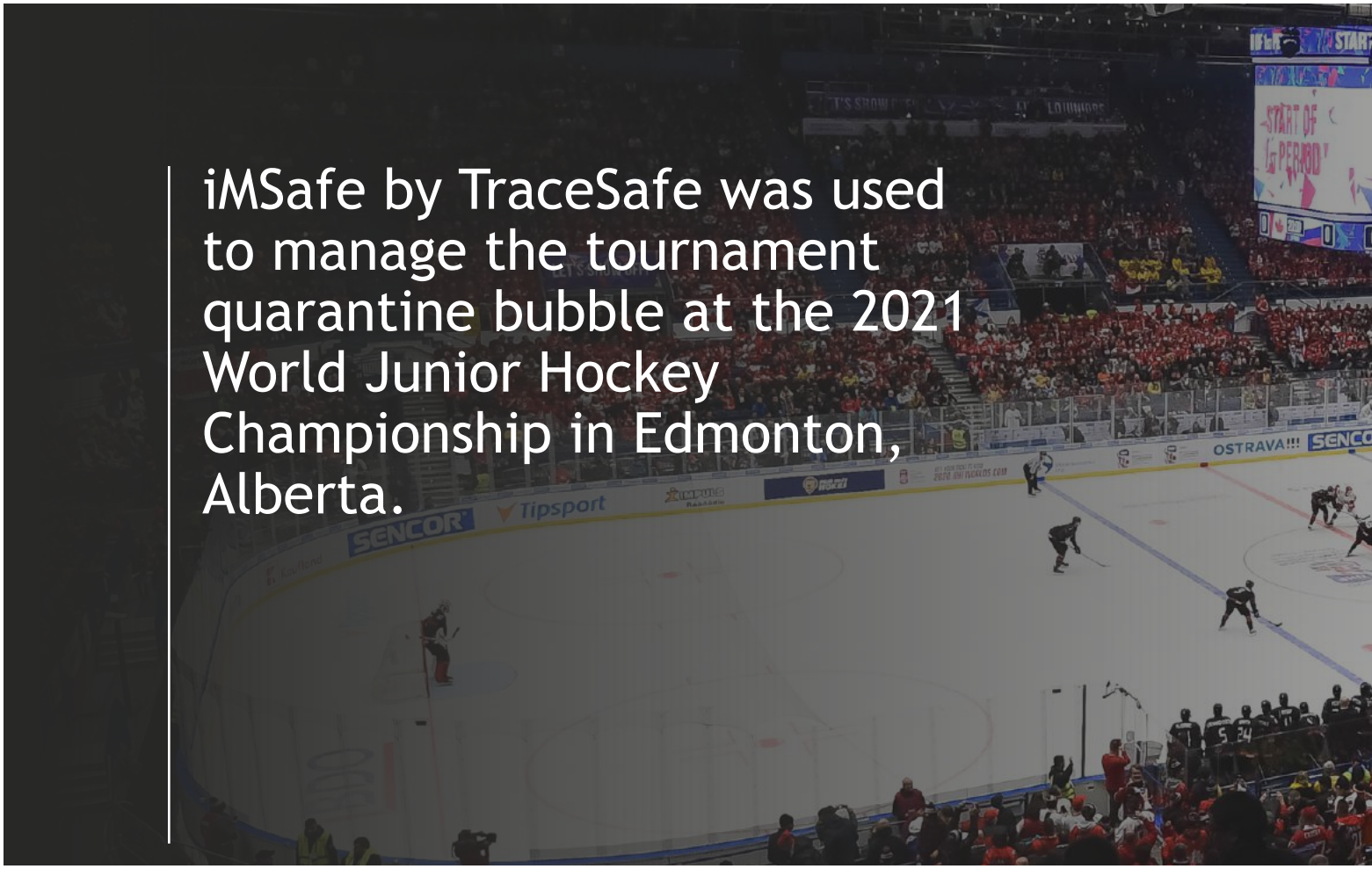
When iMSafe becomes an option for citizens, travellers could choose to quarantine in the privacy of their own home, and taxpayer dollars would not go toward manual enforcement (private security firms and government agents) of a quarantine program with ineffective results.



When a government shows the capacity, expertise and technical knowledge to make decisions in the public's best interest, trust increases.

11. Gozgor, G. Global Evidence on the Determinants of Public Trust in Governments during the COVID-19. Applied Research Quality Life (2021). https://doi.org/10.1007/s11482-020-09902-6

12. TraceSafe Hong Kong Case Study (2020) YouTube, https://www.youtube.com/watch?v=IUmyKaytCZc



iMSafe by TraceSafe was used to manage the tournament quarantine bubble at the 2021 World Junior Hockey Championship in Edmonton, Alberta.

SECTION 7

CONCLUSION

Compliance with public health directives and trust in government go hand in hand. Governments and organizations looking to enforce quarantines need an effective solution that is proven, privacy-preserving, and strikes a balance between fundamental human rights and preventing further spread of COVID-19.

TraceSafe's iMSafe solution has been deployed around the world by governments to manage their quarantine management program, providing centralized alerts, data, and management capabilities. It is built on medical-grade privacy, using Privacy by Design principles and top-grade encryption. iMSafe strikes an efficient balance between privacy and public health concerns, instilling confidence in a government that is transparent, digitally competent and trustworthy enough to lead a nation through a crisis.

Compliance with public health directives and trust in government go hand in hand.

ABOUT THE AUTHOR

Marcin Samiec is the Chief Privacy Officer at TraceSafe Technologies Inc., a global leader in wearable safety technology and connected workforce solutions, where he focuses on delivering the Privacy-First strategy for data protection compliance.

Marcin previously founded PrivacySense.net, a Canadian website focused on educating individuals on their privacy rights and businesses on how to comply with privacy laws like Canada's PIPEDA. With over 50 original articles and guides on privacy, PrivacySense attracted over 30,000 unique monthly visitors and has been referenced in textbooks and privacy and security training resources worldwide.

Prior to founding PrivacySense, Marcin was the Privacy Officer at Checkwell Decision Corporation (now Sterling BackCheck) and led a team of privacy professionals in its global privacy compliance program.