DECONSTRUCTING/PERFORMING THE AMAZON RING SECURITY APPARATUS

Prepared for: Office of the Privacy Commissioner of Canada

Researchers: Evan Light (PhD), Craig Fahner, Ellouise McGeachie, Quinn MacNeil

York University – Toronto Metropolitan University

March 2023

TABLE OF CONTENTS

Abstract

In 2018, Amazon acquired Ring – a start-up company specializing in remote-controlled doorbells with built-in cameras. Since this acquisition, Ring/Amazon have rolled out a plethora of technologies that enable the consumer to easily convert her home into a radically surveillant space.

Today, one can install multiple outdoor cameras including motion-activated spotlight cameras, indoor cameras, sensors that determine when windows and doors are opened, and more. While these capabilities may resemble any of a number of home security solutions on the market since the 1980s, Ring/Amazon's contributions to the market are unique in that they have as much to do with data collection and policing as they do with home security. The Amazon/Ring home surveillance equipment interface conveniently integrates with Amazon "home assistants" *Amazon Echo* and *Amazon Alexa* as well as with police forces. In the United States, Ring/Amazon have signed partnership agreements with some 2000 police forces, providing police with a streamlined mechanism for acquiring surveillance video. There have been discussions around expanding such relationships in Canada, beginning with the Windsor Police Services. There has been sparse scrutiny of Amazon/Ring's relationships with police forces in the United States and no attention paid to what this emerging model of policing means for Canada.

To date, there has also been little critical attention paid to the technical capabilities of this surveillance eco-system in Canada, the legal frameworks it operates within and outside of, and the variety of technologies that are being integrated into them (facial recognition, skin pattern and colour recognition and other forms of biometrics).

Amazon/Ring has further extended its realm of data collection through Amazon Sidewalk, a feature that allows Amazon and Ring devices to connect further away from WiFi routers and therefore deeper into communities to capture data and surveillance footage. This feature has been activated in Ring products without consumer consent and provides automatic network connectivity to nearby devices. This project will examine how the Ring surveillance apparatus watches and tracks people, where the data generated by this

surveillance goes, and the laws and policies that govern these interactions. Using a research-creation approach, we reverse engineered Ring's facial recognition and data collection technology using open-source tools; creating a public-facing interactive narrative that speculatively illustrates the depth of Amazon's integration in surveillant networks.

Project Summary

Deconstructing/Performing the Amazon Ring Security Apparatus critically examines Ring through two central projects:

1. *Enter the Ring: Facing Amazon's Ring of Surveillance* is an immersive art installation wherein gallery-goers are invited to experience facial recognition in real-time with the use of our custom-built facial recognition visualizer. Accompanying the facial recognition experience is a 12-minute video that analyses the Amazon Ring, debunking innocuous advertising campaigns and explaining precisely what Ring owners have gotten themselves into. A six-page, tri-fold gallery guide provides users with further information about Amazon Ring, paraphrasing of critical aspects of the company's *Terms of Use* from legal into everyday language, and facial recognition more generally.

2. *What hath we Rung? Facing Amazon's Ring of Surveillance* is the title of both a reformatted version of this report aimed at policymakers and an academic article in development. In these texts, we document our research and creation efforts, discuss the risks and benefits inherent in Amazon Ring and related technology such as surveillance cameras, facial recognition and artificial intelligence. We propose artistic undertakings such as *Enter the Ring* as an important, innovative method for engaging both the public and policymakers in discussions on complex issues that confront us all with increasing speed.

Original Plans

As with many projects, this one began as an ideal proposal on paper and evolved over the course of many months as experiments were undertaken, research was undertaken, and a research team collaborated for the first time. After a summer of contemplation and experimentation, the team met weekly for 1-2 hours. It should be noted that project lead Evan Light has been on sabbatical and living on Vancouver Island during the course of this project while the rest of the team has been physically in the Greater Toronto Area.

Our original plan for the physical manifestation of this project was the following:

1. Facial recognition visualizer: Press reports and patent filings point towards Amazon/Ring integrating facial recognition technology into components of the Ring eco-system. Exhibit attendees will be invited to have their faces used in a simulation of the facial recognition process. A projection will detail the various ways that data is extracted from human faces and compared to databases using facial tracking and machine learning systems.

2. Surveillance Stories 4 You: Using the faces of exhibit attendees, we will provide a critical perspective on telling stories about surveillance and security.

3. Ring Eco-System Visualizer: Using a mix of specialized software (Touch Designer) and open-source software (Wireshark, Frida, mitproxy), we will provide a real-time visualization of how data is being captured by the Amazon Ring Show Home and where it is being sent.

As we worked to develop them, each of these components changed in important ways due to external factors and changes in strategy.

Challenges and Re-orientations

Amazon Ring Show Home: Our original plan was to build a physical set, a task that would require not only a large amount of physical labour and expertise but would also necessitate sizable long-term storage and complex transportation. In addition, we had great difficulty in recruiting a set builder. These complications led the research team to a more favourable design choice: the use of projection mapping. Projection mapping is a technique that uses specialized software (in this case MadMapper) to project multiple video sources onto multiple surfaces with a single projector, enabling us to display the independent components of our project simultaneously with little physical infrastructure. Thus, we were able to construct a multi-dimensional model home by hanging nine thick plastic sheets of varying size from the ceiling by wood planks and cord; a modestly-priced short throw projector, a Mac mini computer, a customized front door, an Amazon Ring doorbell and various accessories. Thus, the entire exhibit can be somewhat easily transported to other exhibition spaces. The backdrop, rather than being built with actual wood, consists of projections of images of middle-income suburban houses that were generated using the AI-image generator DALL-E. The images have been slightly animated using MadMapper.

Facial Recognition Visualizer

This component developed largely as planned. Based on the open-source package faceapi, it uses open-source datasets to map faces, determine gender, age and affect, and recognize objects that may come into the view of the camera. This component will be further developed to be fully web-based so that the general public can explore it via devices of their choice. In addition, we were invited to demonstrate the facial recognition visualizer (FRV) at a meeting of the International Network of Civil Liberties Organizations where it was received with great excitement and a desire to make use of it in various international jurisdictions.

Surveillance Stories 4 You

Initial plans were to, in part, remix a variety of publicly available Amazon Ring advertising videos and to capture and use digital versions of the faces of gallery-goers to illustrate the power of facial recognition tools and Amazon Ring. This component was adapted substantially due to two reasons. First, in order to capture faces in such a way in an academic context, we would have had to acquire informed consent from everyone participating, making for an onerous experience for all. It was decided to instead make the entire exhibit privacy protective and to limit the use of faces to the FRV. Second, the OPC was concerned that our use of Amazon Ring videos could be construed as a copyright and trademark violation. We acquired our own favourable, if unofficial, legal advice from an expert in Canadian copyright and trademark law. This project is strictly educational and without profit motive and thus falls outside copyright and trademark protections. While awaiting the OPC Legal Services' opinion it was decided to instead develop a script for a voice-over accompanied by on-screen text. A contracted voice actor provides two-thirds of the voicing while the rest has been produced with AI-generated voices using the online suite murf.ai[1].

It should be noted that OPC Legal Services provided an opinion that was in agreement with the one we obtained, but it arrived too close to our production deadline.

Ring Eco-System Visualizer

This component was omitted from the final project for multiple reasons. We had planned to use the open-source application IoT Inspector[2] to attempt to determine where and how Amazon Ring devices collect data. However, as we were preparing to explore its use, the developers announced it would be undergoing a dramatic redevelopment. The initial date for the relaunch of the application was summer 2022, was extended multiple times and is currently set to relaunch in summer 2023. There are no similar open-source software packages available and we plan to conduct this research once IoT Inspector is re-launched. Additionally, attempts to use Privacy International's Data Interception Environment (DIE) to analyze data outputs from the Amazon Ring app proved fruitless as Amazon does not seem to permit installation of their app on virtual phones. As software for conducting this form of analysis advances, we plan to make further attempts.

Audience Reception

Enter the Ring: Facing Amazon's Ring of Surveillance was exhibited at York University's Sensorium Research Creation Studio from 13-17 March 2023. It was advertised on internal email lists at York University and on the email lists of related professional associations. Foot traffic was slow early in the week, providing us with the opportunity to fine-tune a large installation we had not previously constructed and to learn how the FRV reacted to a variety of heights and skin colours. As the week progressed, a number of York professors brought their classes to experience the installation, and members of the general public attended as well. Below is feedback we plan to address or integrate in future iterations of this installation.

[1] https://murf.ai

[2] https://inspector.engineering.nyu.edu/

- The voice we use as the “voice of Amazon Ring” can be characterized as a peppy white male. Some visitors thought this to be counter to our critical engagement with technology that has been shown to have racial and gender bias.
- The AI-generated houses appear to be wealthy suburban homes, precisely the places where one would find Amazon Ring doorbells in use.
- The FRV provides some of the transcript in red text. Some visitors found this to be difficult to read, especially for those with low vision. The font will be changed to improve accessibility.
- People would like to learn more about the exhibit, how it was set-up, how it works, technical aspects, how we got everything together, who did what, who we are.
- People would like to learn more about law enforcement use and FRT (One dark-skinned visitor shared that he was misidentified by FRT in a past police encounter in the U.S. The visualizer didn't detect his face at all, in any type of lighting).
- It is important to have signs outside and inside telling people they are not being recorded or tracked. This was the most frequent question received, even after saying “no” and explaining that exhibit is for educational purposes only, that no tracking or recording is taking place, that the project is funded by the OPC, and that this information is listed in the brochure. Three people decided they'd rather not come in and left because they were too nervous—two of them were people of colour. Any future installations will include signs clearly indicating the aforementioned.
- People would like to know what parts of the video they are watching when each segment starts, whether it's security, monitoring, or convenience. This may be addressed by a title slide before the beginning of each segment.
- An undergraduate student said they were very interested in what we were doing, and asked how they could find a work-study position on a similar project in the future.
- There were many compliments regarding the overall look and aesthetic of the exhibit. It was described as “cool” and “fun”.
- The slight movements of the house were described as “cool” and” creepy”. This refers to mild effects we applied with MadMapper.

- People enjoyed experiencing the night vision setting and making silly faces in front of the camera (with or without lighting). Students and the general public posted photos and videos of themselves testing the visualizer to social media.
- We should install a light atop the door to improve the lighting of people's faces and facilitate a smoother face recognition experience.

Future Plans

Given the positive reactions from visitors, including a representative from the OPC, and from members of the International Network of Civil Liberties Organizations, the research team is contemplating organizing a larger gallery exhibit of surveillance and privacy-related art in Ottawa as a means of engaging policy-makers. We are also in discussions with the Canadian Communication Association to exhibit our installation at their annual conference which will take place at York University in May/June 2023.

Academic Article

A peer-reviewed academic article examining our efforts is currently in development and will be submitted to the Canadian Journal of Communication for peer-review in April 2023. Once published, it will be provided to the OPC.

Abstract & Plans

Enter the Ring: Facing Amazon's Ring of Surveillance is an immersive speculative art installation wherein attendees, should they choose, can have their faces subjected to facial recognition in real-time. Using this installation as a jumping point, we document our research and creation efforts, discuss the risks and benefits inherent in Amazon Ring and related technology such as surveillance cameras, facial recognition and artificial intelligence. We propose artistic undertakings such as *Enter the Ring* as an important innovative method for engaging both the public and policymakers in discussions on complex issues that confront us all with increasing speed. Fundamental to our exploration of Amazon RIng and facial recognition technology (FRT) is the fact that there exist few if any laws to govern the use of these technologies.

As FRT and concomitant technologies such as artificial intelligence develop further, what role is there for the state to govern what are essentially unknowable black boxes? How can artworks such as *Enter the RIng* be used to ponder uses and developments in order to inspire and develop speculative policy, policy that is able to bob and weave with the unknown.

Appendix

Exhibit A: Videos of Exhibit

(Click links to download/view):

Enter the Ring Exhibit – Full Video Sequence

Face Tracking – Shot 1

Face Tracking – Shot 2

Face Tracking – Shot 3

Exhibit B: Brochure

Exhibit C: Poster

Welcome to *Enter the Ring: Facing Amazon's Ring of Surveillance*.

This exhibit has been crafted by a team of researchers dedicated to privacy, equity, and human rights. We use Amazon Ring, a popular home-monitoring device consisting of a doorbell equipped with a built-in miniature camera, to provide an immersive learning space for critical thought and engagement surrounding facial recognition technology and its use in Canada.

The use of this technology has rapidly expanded within the past decade, with facial recognition operating in airports, shopping malls, at sporting events, and more. It has also been used to locate missing persons and solve crimes, while at the same time, being used by authoritarian governments to track, monitor, and detain entire populations.

As you look around, we encourage you to think critically about how technology like facial recognition can potentially impact our lives and freedom of movement, our homes and communities, our judicial system, and the ways in which we interact with and "recognize" each other.

Please note: Your image is not being recorded, analyzed, saved, stored, transmitted, shared, streamed, broadcast, or photographed. This exhibit is for educational purposes only.

This project has been funded by the Office of the Privacy Commissioner of Canada.

CONTACT

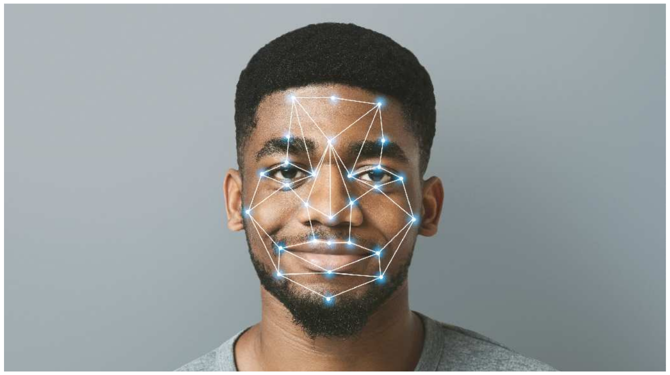
York University & Toronto Metropolitan University
surveillance@glendon.yorku.ca

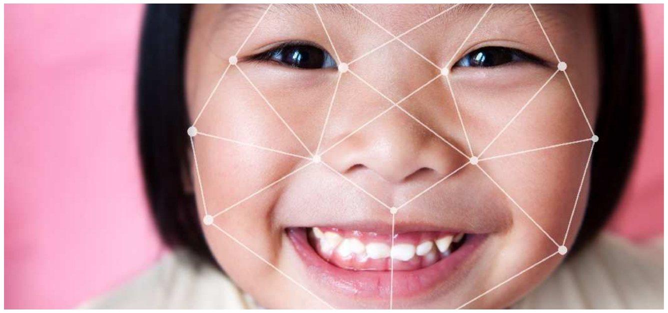
Contact your MP and demand laws for facial recognition now.

This project has been funded by the Office of the Privacy Commissioner of Canaada.

ENTER THE RING

FACING AMAZON'S RING OF SURVEILLANCE





ABOUT FACIAL RECOGNITION

Facial recognition is a type of biometric technology that mathematically maps out an individual's face, and stores the data as a faceprint. This faceprint is stored and later used to verify a person's identity. For instance, some cell phones have a feature that enables users to unlock their device by presenting their face.

In adequate lighting, the technology can produce powerful results with a high degree of accuracy for some groups. However, the technology is not perfect, and is far less accurate when it comes to women, the elderly, persons with disabilities and in particular, people of colour or with darker skin tones. The latter has already resulted in several cases of mistaken identity and persons being jailed for crimes they did not commit.

In China, facial recognition technology has been used to log almost every citizen in the country of 1.4 billion people. China has also used the technology to profile, track, and monitor its Muslim Uyghur ethnic population, detaining over 1 million people in "re-education" internment camps under inhumane conditions.

Recent developments in civil rights and heightened concerns over national security have prompted several American states and cities to ban or limit the technology, or have placed a moratorium on its use until further research is completed and legislation is drafted.

The European Union is also analyzing means to regulate the technology, and to ensure it is not used in ways that may constitute as a non-democratic intrusion into individual's private lives, and mitigates "physical or psychological harm".

In Canada, facial recognition remains unregulated and there are no laws specifically addressing how the technology should or should not be used and by whom.

AMAZON RING

"Convenience", "monitoring", and "security" are the terms Amazon uses to define and market its most popular device, the Ring doorbell. Ring enables users to remotely monitor the inside and outside their homes via smart phone or computer, for things such as visitors or package drop-offs.

Initially launched via a start-up company in 2013, Amazon bought Ring in 2018. The technology has since become the #1 home security device in the world, selling over 1.7 million units in 2021 and making up ~15% or 1/7th of the global market.

But what are we really getting for our money? Is this technology as trustworthy as its alleged to be? Is anyone else listening to or watching the footage? What does Amazon do with all the data it collects from us? Where is it stored? Who might it be shared with?

A 2019 report from news source "The Intercept" claimed that Amazon gave unrestricted access to Ring engineers and executives to watch the live feeds of users' homes, without their knowledge or consent. Some of this footage also included the inside of homes. In 2020, four Amazon employees were fired for improperly accessing and watching users' Ring footage.

Ring is not equipped with facial recognition. However, Amazon does sell this technology to third parties and has been further testing it on sellers who agree to participate in the program.

There is currently no data or evidence proving that Amazon Ring helps to make neighbourhoods safer. The company makes no guarantees of this either, specifically stating: "No guarantees made regarding technology's usefulness, security, or privacy capabilities" (p.13) in its Terms of Service.

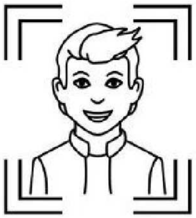
AMAZON RING & YOU

Many people have come to rely on the Ring doorbell as a means of having peace of mind while away from home. While Ring touts convenience and ease of use, it is important to know that there are limitations within the device's terms of service that may affect the user physically and financially.

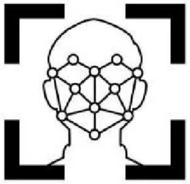
These limitations may not be clear or easy to understand due to the terms being written in complex legal language. Here are a few re-written in everyday language, taken directly from Ring's terms of service:

- Ring makes no guarantees regarding safety, security, usefulness, crime reduction, or privacy. In case of fire, flood, burglary, robbery, or medical emergency, you are responsible (p.11).
- Ring will not contact police, paramedics, or fire services in the event of an emergency—that is your responsibility (p.20).
- Your legal rights to pursue Ring for damages in court are restricted to a maximum of $2500USD or 5x total purchase price of your product(s) as determined by a judge. This remains true for injury, loss of life or property, or loss of income (p.20).
- By using Ring, you have agreed to hold the company "harmless from and against all claims, actions, lawsuits and any other legal action." (p.21).
- If Ring footage is hacked or stolen via malware (malicious software), you are responsible for any consequences and cannot pursue Ring for damages of any kind, even if Ring may be at fault (p.37).
- Ring has the right to modify their terms of service at any time.

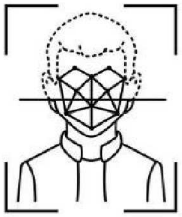
HOW FACIAL RECOGNITION WORKS



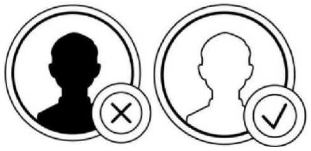
CAPTURE



EXTRACT



COMPARE



MATCH

Facial recognition works by capturing the image of a person's face and extracting facial measurements. These measurements are saved as a faceprint, which can then be compared and matched with others to verify an individual's identity.

CAPABILITIES & LIMITATIONS

Facial recognition can detect a person's age, gender, and facial expressions. It is used to facilitate smoother passage through airport customs, mitigate identity theft or fraud, and to locate missing people. The technology has an accuracy rate of up to 90% but this is inconsistent and varies widely across demographics.

Vulnerable groups such as women, people of colour, and persons with disabilities are more likely to be misidentified. Facial Recognition consistently performs poorest on Black women between the ages of 18-30, with error rates up to 34% higher than other demographics. Women of colour are the second group with the highest inaccuracy rates.

Facial recognition algorithms can also be bias. As algorithms are mainly trained on detecting the faces of white or fair-skinned males, people falling outside of this scope tend to have higher inaccuracy rates.

Some companies have been caught using facial recognition technology on Canadians without their knowledge or consent.

In 2020, the CBC published an article revealing that commercial real estate company Cadillac Fairview was being investigated by the federal, Alberta, and British Columbia privacy commissioners. The company had inserted facial recognition cameras into its digital information mall kiosks, capturing over 5 million faces. The data was supposedly used for marketing purposes.

Cadillac-Fairview owns 18 malls in major cities across Ontario, British Columbia, Alberta, Manitoba, New Brunswick, and Quebec. This list includes the Toronto Eaton's Centre, Sherway Gardens, the Rideau Centre, and CF Carrefour Laval .

Since the investigation, Cadillac-Fairview stated that it has removed all facial recognition technology from its properties and deleted the data it collected.

AMAZON RING & PRIVACY

Amazon Ring collects the following information about you, according to the company's privacy policy (p.2-5):

- Contact Info: Full name, phone number, and postal code.
- Payment Info: Full name, (partial) credit card number, expiration date, and security code. Amazon only retains the last 3 digits of your credit card. Your full credit card number is managed by an unnamed third party.
- Social Media: Information about you from social media and payment services such as FaceBook, Instagram, and PayPal. This occurs if you sign-in to your Ring account through social media or if you share your Ring footage on social media.
- Ring Footage: All of your Ring content is captured and recorded, including video, live streams, images, comments, and data. Your Ring may also collect information from other devices connected to your Ring.
- Personal Data: Some information collected about you is shared and/or sold to unnamed third parties and advertisers.

In 2021, Amazon turned some of its users' Ring footage into a comedic, reality TV style show called "Ring Nation". It is similar to the blooper show "America's Funniest Home Videos". This allowed the company to profit from the user recordings they obtained for free. The series has been condemned by activist groups along with American Senator and privacy advocate, Ed Markey.

A CNBC article in August 2022 quoted Markey as saying:

"With Ring Nation, Amazon appears to be producing an outright advertisement for its own products and masking it as entertainment [...] The Ring platform has made over-policing and over-surveillance a problem for America's neighborhoods, and its normalization is no laughing matter."

PROS & CONS OF FACIAL RECOGNITION

- Locate Missing Persons
- Help Solve Serious Crimes
- Facial Recognition Databases Can Be Hacked
- Non-Democratic Intrusion into Public & Private Life
- There are currently NO Laws or Limitations on the Use of Facial Recognition in Canada

POTENTIAL IMPACTS

The unregulated use of facial recognition technology presents a state of uncertainty for our society, and many urgent questions:

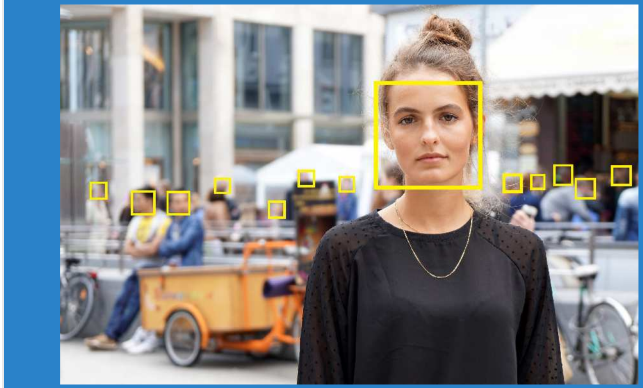
Who can use this technology, for what purpose, and why? What protections exist if faceprints are stolen or misused by malicious actors? How do we manage companies using facial recognition without telling their consumers? Should law enforcement require a warrant before accessing this data?

Should you have the right to know when your facial profile is being captured or collected? Should parents have the right to know when facial recognition is being used on their child(ren)? How might this technology impact vulnerable groups?

It is possible to protect the rights and freedoms of Canadians and enjoy the benefits of facial recognition technology in a fair, ethical, and transparent way.

But we need laws to help make this a reality.

Contact your MP today and tell them to introduce legislation addressing facial recognition technology and the privacy rights of Canadians.



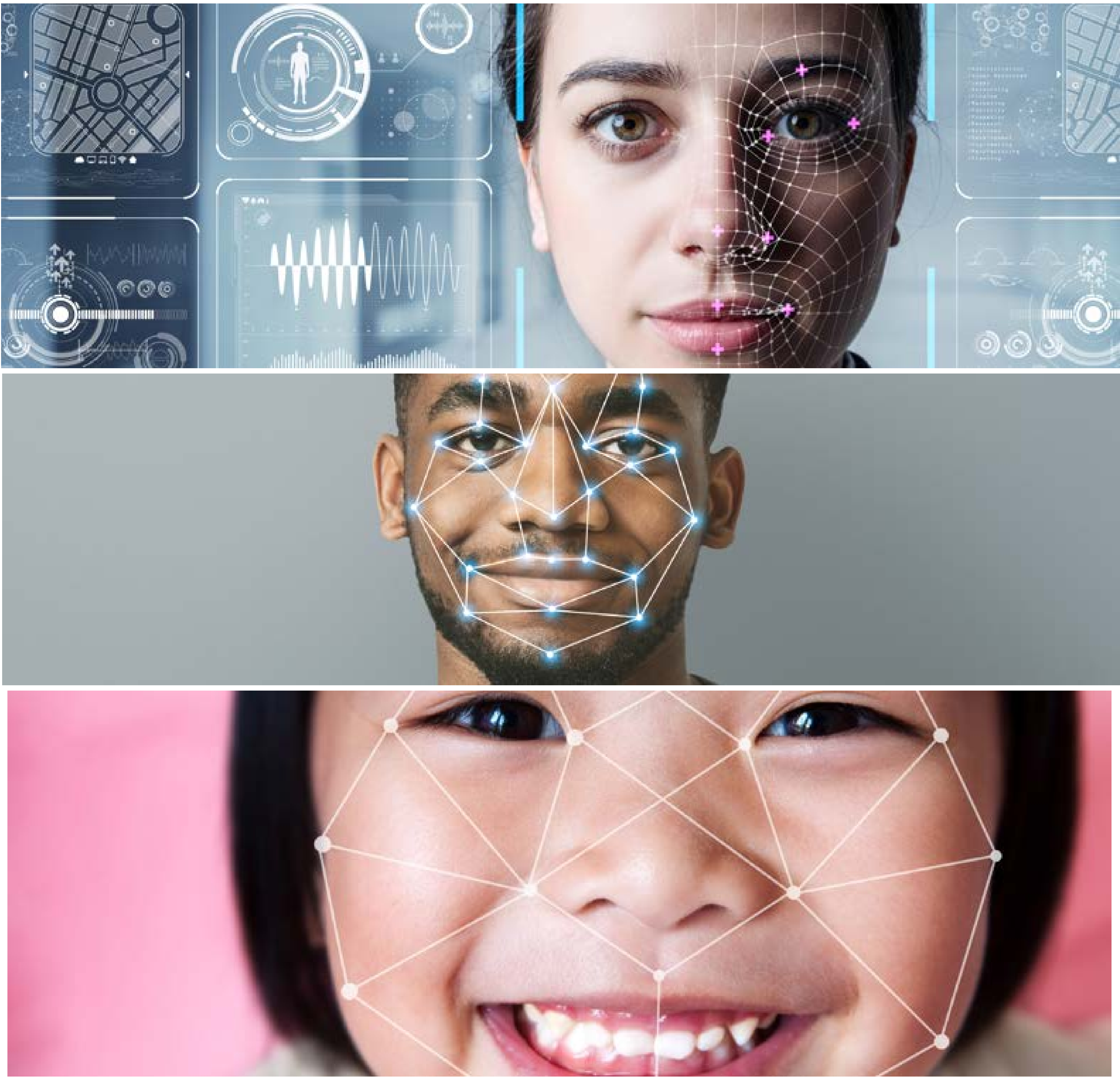
POTENTIAL BENEFITS OF LEGISLATION

- Safeguard Democracy, Peaceful Assembly, & Vulnerable Groups
- Protect Your Privacy
- Improve Your Legal Rights
- Promote Fairness
- Make Companies & Organizations Accountable for their Actions

ENTER THE RING:

Facing Amazon's Ring of Surveillance

An immersive, interactive exhibit examining the Amazon Ring doorbell, privacy, and the implications of facial recognition technology use in Canada.



YORK UNIVERSITY (Keele Campus)
MARCH 13-17, 2023 10:00AM-6:00PM

ROOM 326, SENSORIUM FLEX SPACE FOR DIGITAL ART & TECHNOLOGY
Goldfarb Centre for the Arts, 86 Fine Arts Road
Admission: FREE

This project has been funded by the Office of the Privacy Commissioner of Canada