WHITE PAPER

The Case for Scaling Computer Vision

# Enhancing Safety in Uncertain Times

04 / 2020

# TABLE OF CONTENTS

# I. Introduction

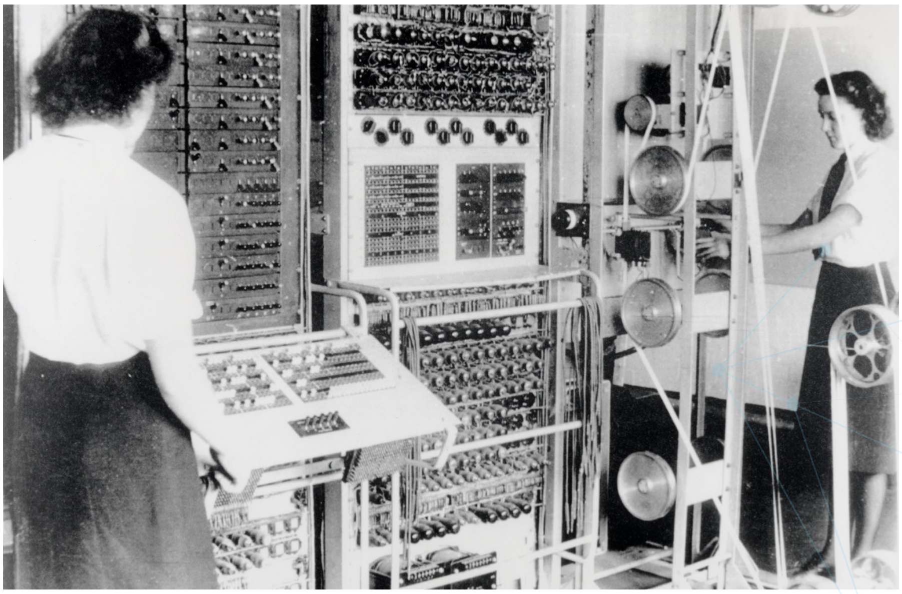
Necessity, as Plato said approximately 2,400 years ago, is the mother of invention. The Covid-19 pandemic has presented an unprecedented necessity for invention, and the unified action of mankind coupled with invention is critical to overcoming this threat. McKinsey & Co writes in a recent article that, "technology is on the front lines of this crisis. Many of the changes reshaping how we work and live—from employees working remotely to consumers shifting their shopping online—rely on technology." An even more fundamental role of technology in the pandemic is saving lives today and scaling the innovations driven by current necessity to protect mankind in the future. Computer vision is a technology that can help to reduce the spread of Covid-19 today and protect mankind in a variety of ways going forward, and now is the time to scale it.

The pandemic has widely been compared to a war. War is defined by the Oxford Dictionary as "a state of armed conflict between different nations or states or different groups within a nation or state." While this pandemic is not by definition a war, there are parallels in terms of how technological innovations developed during wartime can help to end the current crisis and protect and improve lives when this threat is defeated.

British wartime radio navigation inventions helped fighter pilots find targets and became the foundation for the Instrument Landing System (ILS) that helps planes navigate and land today. Pressurized cabins allowed us to fly comfortably at higher altitudes. Modern radar was also developed during WWII,

and it led to the miraculous convenience of the microwave oven. Missiles and the advanced fuel and guidance systems that powered them enabled mankind to set foot on the moon. Canadian scientists developed anti-fog windshield fluids and helped pioneer synthetic rubber. The introduction of the jet engine in 1944 accelerated the end of the war, and today these engines fly humanity around the world. Though penicillin was discovered in 1928, it was wartime necessity that scaled its use, which is credited with saving tens, if not hundreds, of millions of lives since then. And without question, the most transformative technical capability born of war is the computer. Developed by British codebreakers to support cryptoanalysis, a series of computing devices collectively known as Colossus was the groundbreaking forefather of the computers that we largely take for granted today.

Every public and private entity that serves or supports people during this new war has a responsibility to apply technology to enhance safety. Businesses, organizations, and governments can make the world safer, more secure and more accessible for the people they employ, protect and serve through the use of intelligent computer vision. As the current threat eventually subsides and the world returns to work, intelligent computer vision will continue to enhance safety and will ultimately become part of daily life that will one day be taken for granted.



*A Colossus Mark 2 codebreaking computer being operated by Dorothy Du Boisson (left) and Elsie Booker (right), 1943*

[2] https://en.wikipedia.org/wiki/Colossus_computer

# II. Three Pressing Safety Risks

The rising threat of coronavirus has elevated existing risks and made them intolerable. Having to touch surfaces in high-traffic, public settings to gain secure access to space is intolerable. Relying only on people monitoring screens to identify threats is intolerable and also unfair to the hardworking people in security rooms. The risk of fraud in accessing vital services via personal devices is intolerable and presents even greater societal disruption risk if public organizations, financial services and healthcare providers cannot securely deliver remote services.

## 1 THE WORLD RUNS ON TOUCH

Accessing much of the world today depends largely on human touch, and touching surfaces and then absent-mindedly touching our faces can communicate Covid-19. As the BBC reported recently, "there are now some familiar scenes in public places around the world – people trying to open doors with their elbows, commuters studiously surfing their way through train journeys to avoid grabbing a handle, office workers rubbing down their desks each morning."[3] Local shelter-in-place mandates have eliminated the nearterm need to commute and wipe down work spaces, but as it is deemed safer to open local and national economies, corporate, commercial and public spaces and services that require some form of touch to enter or authenticate identity must find ways to reduce the need for surface contact.

Touch ID and fingerprint authentication are used globally by both public entities and the private sector despite hygiene and security limitations, but organizations on the front lines of enhancing safety are beginning to seek alternatives.  The New York Police Department recently stated that it would "explore other options if fingerprint scanners need to be taken offline for an extended period of time".[4]

## 2 HUMAN VISION ALONE CANNOT CATCH EVERY THREAT

In addition to reducing the need to touch surfaces to gain secure access, it is critical to enhance human efforts to identify persons of interest (POI). Augmenting manual identification - human teams watching screens - with technology is important for three important reasons.

In certain countries and in certain environments such as hospitals and public spaces, identifying people who have been quarantined, are known carriers of Covid-19 or have been in contact with known carriers can help to protect medical staff, authorities or public servants who are essential for maintaining services to citizens. It is equally important for restoring the economy to be able to identify

[3] https://www.bbc.com/future/article/20200317-covid-19-how-long-does-the-coronavirus-last-on-surfaces

[4] https://findbiometrics.com/biometrics-news-nypd-hq-ceases-use-fingerprint-authentication-slow-coronavirus-031107/

known carriers who have recovered and are safe to move freely and return to work. Countries and organizations who are able to carry out "benevolent surveillance" with the support of technology will fare better in this crisis and recover from it quicker.

There is no precedent in modern economic history for the cause and immediacy of the recession the world is facing, but there is sadly precedent that crime rises in economic downturns according to a report by Congressional Research Service (CRS), the organization dedicated exclusively to providing analysis to the US Congress.

> “*...some research suggests that other economic variables, such as gross domestic product (GDP) or gross state product (GSP), as well as consumer sentiment, could flutage more closely with crime rates and could thus serve as better proxies for evaluating the relationship between the economy and crime.*[5]”

While video infrastructure and camera setups are commonplace among virtually every building and public area to prevent risk, less than 5% of video ever gets analyzed.[6] This statistic, while concerning, isn't surprising given the manpower required to monitor content. How much safer would a hospital, a retail store, a facility with critical infrastructure such as a data center, or an ATM network be if public and private entities alike had the ability to analyze 100 percent of video footage? It's simply unrealistic and unfair to expect human vision alone to identify threats to safety.

## 3 THE RISE IN REMOTE SERVICES AND THE RISK OF DIGITAL FRAUD

Before COVID-19, online digital services such as telemedicine or online banking were ancillary benefits to customers and just another channel for businesses. Today they're the lifeline for the survival of industries and can be the literal lifeline for people seeking medical care.  Healthcare IT News reports that, "as this public health crisis continues to escalate..., telemedicine is quickly gaining recognition as a critical tool to slow the spread of COVID-19".[7]

At the same time, digital fraud and scamming is rising in lockstep with the increased reliance on remote services. CNN[8] reports that fraud patterns are mirroring the 2008 financial crisis. Organizations that have rapidly democratized access to their services through digital channels must take action now to safeguard their customers and their own assets from fraud and hacks. Making it as safe to access a service from a customer's living room as it is at a branch or doctor's office is suddenly essential.

[5] https://fas.org/sgp/crs/misc/R40726.pdf

[6] "Digital Disruption Profile: CV Sharpens Focus on AI Strategy",

[7] https://www.healthcareitnews.com/news/telemedicine-during-covid-19-benefits-limitations-burdens-adaptation

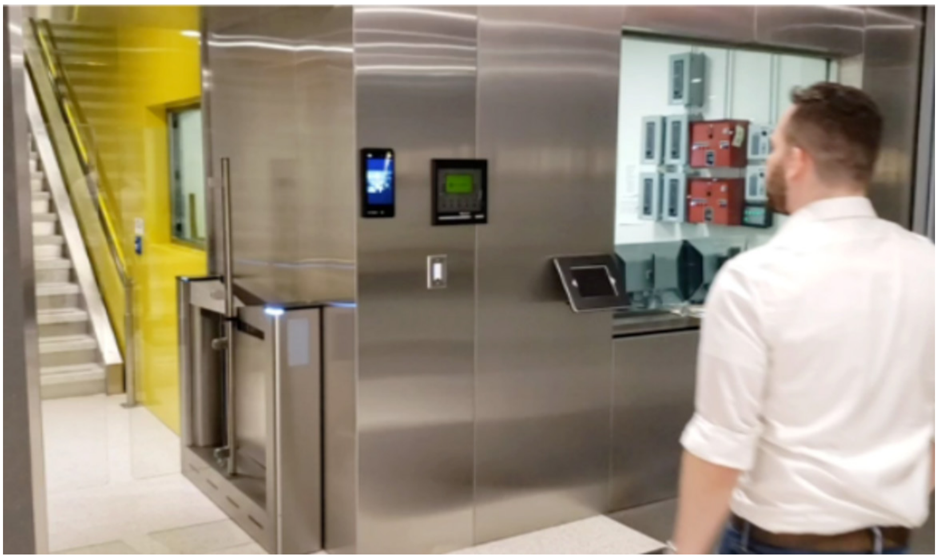
[6] https://www.cnbc.com/2020/03/20/coronavirus-scams-on-the-rise-mimic-fraud-in-2008-financial-crisis.html

# III. Three Key Computer Vision Capabilities

In a March 2018 report, Gartner's Nick Intelbrecht writes that, "the ability of organizations to apply and exploit computer vision to capture value and generate insight from their own video/image data assets will become a question of competitiveness and ultimately survival within the next 10 years.[9]" That timeline is likely accelerating. Touchless access control, visual intelligence for security and remote authentication and verification will help the public and private sectors to enhance safety during this challenging time. Beyond the crises these core computer vision capabilities will, in Nick's words, bring "greater levels of automation resulting in improved quality, speed and reliability, improved decision support, enhanced customer experience and reduced cost."

## 1 TOUCHLESS ACCESS CONTROL

Touchless access control is a computer vision capability that uses opt-in facial recognition to unlock turnstiles, operate gates or open doors to spaces they are authorized to enter. It entirely eliminates the need to touch surfaces or continuously touch a key card. It is similar to parking garages that utilize computer vision to scan license plates to let registered cars enter the facility. In addition to enhancing safety, touchless access control also reduces lines and waiting times. For property managers and owners, the capability increases the security of buildings by eliminating the ability to "tailgate," which is when uninvited individuals follow people with access into a space.



[9] Gartner, Nick Ingelbrech, Digital Disruption Profile: CV Sharpens Focus on AI Strategy, 20 March 2018

**How does touchless access control work?**

- A user -uploads images of people with approved access or syncs current access control with the new system
- An intelligent edge device or existing visual sensors paired with computer vision software are positioned at external and internal entry points
- Recognition software allows entry for people upon arrival

**What to look for in a state-of-the-art touchless access control system:**

- Accurate and fast recognition to prevent people from waiting and congregating at checkpoints
- Anti-spoofing for maximum security
- Seamless integration to existing access control system and database
- Can leverage existing infrastructure to reduce cost and speed of implementation
- Compatible and compliant with GDPR and privacy regulations

## 2 VISUAL INTELLIGENCE FOR SECURITY

Visual intelligence is a computer vision capability that adds AI-driven automated recognition of faces, bodies and objects to manual recognition and detection efforts. It is the broadest of the three core computer vision capabilities, including automated watchlist alerting and intelligent quadrant control.

Automated watchlist alerting can be used by any industry to identify known persons of interest (POI) as well as to identify people who have come in contact with POIs. While this capability originated in defense, visual intelligence systems are commonly used by retail businesses to identify known shoplifters to help reduce loss.

Real-time video analytics are essential for threat prevention, and forensic video analysis allows users to review video data from the past. By uploading an image into a visual intelligence system that's connected to your video management software, users can "search backwards" - even just by physical attributes s, like "red hat" or "eye glasses" - and find sightings of a POI or identify the people who had close contact with POIs. This capability has not only been proven for preventing crime and solving crime, it also has significant potential in supporting viral quarantine efforts and identifying potential exposure risks based on visual evidence of contact with known carriers.

Visual intelligence can also be used to create digital barriers or to prevent access to certain areas by unauthorized people. This capability is also referred to as intelligence quadrant control (IQC). IQC can also be used to prevent access to specific offices to, for example, ensure compliance in banking, and it can be used to add security to sensitive areas of a facility. It can utilize existing camera infrastructure or be activated with smart tablets.

**How does visual intelligence work?**

- A user enrolls a list of POIs or authorized people
- Visual intelligence software is connected to existing cameras and the video management system (VMS)
- User receives automated watchlist alerts when the system detects POIs

**What to look for in a state-of-the-art visual intelligence system:**

- Accurate face and body recognition and real-time alerts in complex situations and challenging environments
- Agnostically leverages existing security infrastructure
- Easily scalable to support multi site environment
- High number of video streams per graphical processing unit (GPU) to maximize speed and efficiency
- Compatible and compliant with GDPR and privacy regulations

## 3 REMOTE AUTHENTICATION AND VERIFICATION

Remote authentication and verification is a computer vision capability that can be embedded into mobile apps to use a device's camera to accurately prove a person's identity. Some banking and healthcare apps are already using this capability to reduce the risk of fraud in digital service provision, and a growing number of services are validating a person's identity via mobile apps for faster, more secure admittance or onboarding on site. Most companies use a software development kit (SDK), which provides configurable capabilities in an installable software package.

If a consumer is accessing medical records, transferring money to a friend, buying a ticket to a concert, opening a bank account, purchasing a plane ticket, ordering equipment or any number of other transactions, digital verification makes the service safer on both ends.

**How does remote authentication and verification work?**

- User takes a picture of government ID that includes a photo
- User takes a short selfie video
- System checks for liveness and validates the identity of the user against the government ID and the service provider's database.

**What to look for in a state-of-the-art remote authentication and verification system:**

- Accurate and fast recognition
- Passive anti-spoofing/liveness detection, which ensures that a face is actually attached to a living, breathing person
- And SDK that is device, OS and app agnostic
- Easily scalable to support millions of users
- Compatible and compliant with GDPR and PSD2

Instructions
Take a photo of your face. Make sure to fill the square and ensure adequate lighting
WELCOME!
100%

# IV. How Computer Vision Enhances Safety in Higher Risk Verticals

While every organization committed to protecting people, places and things can benefit from computer vision, there are certain industries that have a more pressing need for enhancing safety. The following industry snapshots list the common safety risks and key computer vision capabilities by vertical.

## HOSPITALS

| | Safety Risks | Enhanced Safety Capabilities |
|---|---|---|
| 1 | Staff exposure | Intelligent Quadrant Control<br>• Enforce digital barriers for quarantine |
| 2 | Identify exposure risk | Automated Watchlist Alerting<br>• Onboard & authenticate patients via mobile for secure onsite admittance<br>• Identify recidivism |
| 3 | Operational friction | Touchless Access Control |
| 4 | Care continuity | Remote Authentication & Verification<br>For digital onboarding and access |

## BANKING, FINANCIAL SERVICES AND INSURANCE

| | Safety Risks | Enhanced Safety Capabilities |
|---|---|---|
| 1 | Legacy biometric access control | Touchless Access Control |
| 2 | Heightened perimeter security risk | Automated Watchlist Alerting |
| 3 | Heightened interior access control risk | Touchless Access Control |
| 4 | Heightened digital fraud risk | Remote Authentication & Verification<br>For digital onboarding and access |

## RETAILERS

| | Safety Risks | Enhanced Safety Capabilities |
|---|---|---|
| 1 | Safety risk of touching secure entry points | Touchless Access Control |
| 2 | Heightened risk of loss as economic impact worsens | Automated Watchlist Alerting |
| 3 | Control employee access to secure areas (e.g. storerooms) | Intelligent Quadrant Control |

## DISTRIBUTION CENTERS

| | Safety Risks | Enhanced Safety Capabilities |
|---|---|---|
| 1 | Legacy biometric access control | Touchless Access Control<br>Rapid onboarding of new workers |
| 2 | Heightened risk of loss | Automated Watchlist Alerting |
| 3 | Heightened interior access control risk | Intelligent Quadrant Control |

## DATA CENTERS/CRITICAL INFRASTRUCTURE

| | Safety Risks | Enhanced Safety Capabilities |
|---|---|---|
| 1 | Legacy biometric access control | Touchless Access Control |
| 2 | Heightened perimeter risk | Automated Watchlist Alerting |
| 3 | Prevent internal access to secure areas | Intelligent Quadrant Control |

### STATE AND LOCAL GOVERNMENT

| | Safety Risks | Enhanced Safety Capabilities |
|---|---|---|
| 1 | Difficult to enforce quarantines | Automated Watchlist Alerting<br>• Onboard tested / quarantine lists<br>• Identify, geo-track and geo-fence |
| 2 | Avoid contact with people who must be identified in the field | Intelligent Edge Devices<br>• Real-time, touchless identification through mobile device |
| 3 | Difficult to track potential historical exposures | Automated Forensics & Timeline Tracking |
| 4 | Delivering public services digitally | Remote Authentication & Verification<br>For digital services |

## V. About AnyVision

AnyVision is a leading provider of each of the capabilities you learned about in this paper. At AnyVision, our mission is to dedicate our core computer vision technology, our expertise and our resources to supporting the organizations and businesses on the front lines of enhancing safety. Since our commercial launch after years of academic research, data-driven organizations have used AnyVision's visual intelligence capabilities to improve operational performance, reduce risk and optimize customer experience. Our software makes any camera smart, and our AI-driven recognition technology helps people protect, optimize and streamline spaces all over the world.

Contact us to talk with an industry expert or to schedule a remote demo of our intelligent computer vision capabilities.

For more information please contact us at: info@anyvision.co