BACKGROUND GUIDE FOR UNGA-DISEC

Agenda-**Evolution of Surveillance Technology for Security Purposes.**

Security is so much more than just table stakes for today's digital business: it goes to the heart of trust in the relationship you build with your customers. High profile breaches and increased public awareness of security and privacy issues have resulted in a loss of trust. We need to rebuild. At the same time, the scale and sophistication of threats grow by the day. The only way to stay ahead of the curve is through the implementation of multidisciplinary security practices that combine continuous delivery with a focus on privacy and security in depth.

Surveillance technology is used to monitor individuals' digital and physical actions and communications. Common forms include data-gathering apps on smart phones, and facial recognition software in smart security camera systems.

Surveillance technology is ostensibly used to improve workplace safety, monitor employee productivity, inform market research, and increase protection for valuable assets. But it can often cross the line, becoming intrusive rather than protective.

The term 'surveillance technology' encompasses any digital device, software or system that gathers information on individuals' activities or communications. Video surveillance

is common, and technology advancements mean that audio and images can now be analyzed in greater detail and with greater accuracy. Today, tools for collecting and sharing data have become a new, nearly imperceptible form of surveillance. Our smart phones, for example, produce and hold huge amounts of personal data — including whom we talk to, where we go, our internet browsing history, our social networks, and more. This data can be collected and analyzed to provide insights into consumer behavior or employee activities. But it can also intrude on people's rights to privacy and could put your enterprise at risk of legal and compliance issues.

Surveillance technology is now cheaper and more widely available than ever. And when applied ethically, with high levels of transparency, it can bring big business benefits. Workplace video surveillance, for example, can provide insights into employee behavior and operations, helping you drive productivity, ensure workplaces are safe, and spot inefficiencies in your processes. Collecting consumer data can also help you improve nearly every aspect of your business, providing deep insights into your customers' behavior, the demographics you appeal to, and what exactly they want from your company and its products. There is a dark side to surveillance technology. It's everywhere — and as the technology becomes more easily available, it's difficult to prevent your data from being collected, or your face being saved in an unknown database. This raises a lot of privacy concerns, threatens civil liberties and increases the risk of blackmail, coercion, or discrimination. There's no way for individuals to know what data is being collected, where it's stored, or how it's being used. And at the moment, there's little legislation to protect individuals, because the technology is advancing too fast for regulators to keep up. An exhaustive legal review on the utilization of surveillance technology is recommended for companies to reduce the risk of compliance issues. There are plenty of applications where surveillance technology can benefit businesses. Amazon, for example, has just released a new workplace surveillance tool called AWS Panorama, which analyzes footage from security cameras to monitor workers' health and safety. For instance, it can detect when employees aren't following social distancing rules, and it can offer valuable insights into operational efficiency and the quality of the employee experience.

Facial recognition technology matches human faces from digital images or videos to those stored in a database of 'known' faces. It is commonly found in authentication systems — for instance, in some models of Apple's iPhone. But the technology can also be found in surveillance systems.

Broadly speaking, facial recognition is a system of matching a human face captured in a digital image or video stream to database records.

These systems have existed for decades but recent improvements in pattern recognition have turbocharged interest in facial recognition systems.

Typically, facial recognition is treated as a method for authentication. That said, there is growing interest in some subsets of facial recognition, such as expression recognition — where the aim is to recognize whether a subject's emotional state. This technology is being used by some retailers to gauge customer interest in their products.

As an authentication system, facial recognition is convenient and touchless — which may appeal to some.

And some companies — for instance retailers and airports — have trialed the technology for security purposes.

While the systems can be highly effective in perfect conditions, they tend to be less reliable when in real-world conditions, with crowded environments, variable lighting and often less-than-ideal camera angles.

More worryingly, many facial recognition packages are poor at correctly identifying faces of anyone other than <u>white males</u>. Given they're often used in surveilling crowds, it's not surprising that many people have concerns over the use of the technology.

The technology is also readily defeated. People not wishing to be identified can wear face masks or paints.

One of the most widely used applications of the technology is to unlock smartphones — so it is familiar to many. It can also be found in surveillance systems at airports, in shops and deployed by law enforcement.

Another type of surveillance security that has emerged is touchless interaction.

A broad range of different ways to interact with devices without having to physically touch them.

The COVID pandemic has heightened interest in input methods that don't require users to physically interact with a device in order to control it. This encompasses a variety of input methods, including voice and gesture recognition.

A range of techniques — such as voice and gesture recognition — that enable users to interact with devices without needing to physically touch them.

Many consumers are already familiar with using voice commands to control digital assistants, such as Siri and Alexa. Similarly, many cars come with voice-enabled controls, some are even trying out gesture controls.

The COVID pandemic is likely to have heightened interest in touchless interactions — many of us harbor concerns about using public screens, which are difficult to sanitize.

As technology becomes more pervasive in our lives, the old notion of input via a keyboard becomes increasingly anachronistic. Touchless interactions could, in many circumstances, help you deliver a better customer experience — according to one study 59% of consumers prefer using voice-based interfaces in public places such as shops, banks, and government offices. Where you have devices operating in public spaces, customer concerns over sharing interfaces is likely to heightened for some time.

Many of today's back-end systems were designed to capture physical data entry. If you were to, say, switch to a voice-based ordering system, you need to think about how you capture that information and design that interaction. Will you need to refactor existing systems to allow for touchless interactions?

Currently, many touchless interfaces are being developed independently. For something like gesture control, consumers may be less willing to adopt if there isn't some standardization on what actions gestures are likely to produce.

And as of today, much of the technology is imperfect. Voice recognition often fails in noisy environments; gesture controls aren't always accurate in poor lighting.

Touchless interactions such as voice control are a common method of interacting with home gaming systems, digital assistants and in-car infotainment. And smartphones, with their pinch-to-zoom control, or swiping left have introduced many consumers to the ideas of gesture control.

There's likely to be increased interest in touchless interactions for some time to come.