EXECUTIVE SUMMARY

Wearable technologies are revolutionizing the way we understand and manage work.

On the ground information about the conditions and context of work is no longer limited to verbal feedback or post hoc reports, but can stream directly and immediately from a sensor-enriched workforce. This allows for faster **detection**, **prediction**, and **analysis** across many industrial workplace settings. From activity trackers that measure wellness information, to unique devices that predict musculoskeletal disease and measure vibration exposure – these are just some of the devices becoming more common in today's workplaces.

While tracking the productivity and health and safety of employees is not new, many are concerned about the potential for these devices to extend various powers of surveillance inside the body. Previous research has provided some indication of how employers are using wearables and the data produced by them; but to date, there has been little discussion of the privacy implications of these devices, let alone in the Canadian context. To address this gap, we examined the technical and informational capabilities of currently available wearable technologies.

Our research uncovered:

- **Over 420 wearable devices** currently available for workplace applications;
- **Nine different device types**: fitness trackers, smart watches, body sensors, smart glasses, body cameras, smart clothing and accessories, virtual reality headsets, dosimeters, and other devices;
- **25 different sensors** helping to illustrate the ways the body and its surroundings are capable of being monitored and rendered as information, and;
- **14 workplace use cases** including: corporate wellness, manufacturing, health and safety, and customer service.

Marketed simultaneously to benefit and empower the user, to increase productivity and efficiency, and to enhance information and communication capabilities by more closely monitoring the conditions and context of work, these personal devices bring renewed importance to earning employees' trust and confidence. The path to earning that trust will be **transparency and accountability** in how wearables are being implemented – necessitating an informed and proactive approach to privacy concerns.

The privacy implications of wearables extend far beyond concerns with how data is collected or handled; what happens after the data is collected also matters. Important questions remain: Can it be **combined** with other information? What about **metadata**? Is the type of information **susceptible** to other uses, beyond the initial purpose?

While there are many organizational procedures and federal and provincial privacy laws designed to protect privacy, the status of information produced by wearables in the workplace remains unclear. Although organizations typically have policies for how employee generated information is controlled, these differ across workplaces and industries, and are grounded in the legal and regulatory realities in which they operate.

To help companies, decision makers and all stakeholders navigate the privacy implications of wearables in the workplace, they should keep in mind the following key recommendations:

1. **Accountability:** When considering implementing wearables in the workplace ensure personal information is handled appropriately by designating and making known an individual responsible for oversight.
2. **Identify the Purpose:** Ensure all purposes for which information collected by a wearable are documented. Provide employees with advanced notification of any new purpose through means that are not easily dismissed or ignored.
3. **Consent:** It is best to always obtain consent. When notifying employees about the purpose of any new technology, be specific about how information will be transferred or disclosed, including mentioning any third parties who may have access to the data for processing. Different privacy laws apply when data is transferred across provincial or national borders.
4. **Limiting Collection:** Avoid unnecessary or indirect collection of information via wearable devices; in some cases, it is better to minimize what employers have access to and can see.
5. **Limiting Use, Disclosure & Retention:** Employers should only retain information sourced from a wearable for a period defined by organizational guidelines setting out retention and destruction procedures.
6. **Accuracy:** Organizations are obligated to ensure that the information collected and used is accurate, complete, and up-to-date as necessary. Rather than fully entrust accuracy to the devices' capabilities, employees should also be allowed to calibrate the accuracy of the wearable's data portrait.
7. **Safeguards:** Organizations should consider conducting a privacy impact assessment prior to implementing wearables. The privacy impact assessment can help determine the extent of the safeguards needed to protect any personal information, such as the need for physical, organizational, and technical barriers to conceal and/or anonymize wearable datasets.
8. **Openness:** Be open about how information is managed and who is responsible. This information should be readily available, easy to understand, accessible, and ideally, posted in areas frequented by employees.
9. **Access:** Employees should have the ability to access data for the purpose of challenging the accuracy or completeness of the information, especially when the information from a wearable is used to evaluate their performance.
10. **Challenge Compliance:** Ensure employees can initiate a complaint and make this known as part of informed consent. Complaint protocols should be simple, easy to access, and cause no undue harm to the employment relationship (i.e., an employee cannot be terminated for lodging a complaint).

The key take away of this report: Taking time to consider privacy before implementing a new technology should no longer be viewed as stifling innovation, but as a new opportunity to differentiate and promote the strengths and competitive advantages of Canadian privacy rights.

Wearables do more than enhance work and empower workers, they offer the chance to take privacy into our own hands.

Wearables in the Workplace

425 WEARABLE DEVICES AVAILABLE TODAY...

28% FITNESS TRACKERS
Steps, Calories, Distance Travelled

25% SMARTWATCHES
Notifications, Location Tracking, Mobile Payments and Authentication

13% BODY SENSORS
Heart Rate, Body Temperature, Fatigue/Stress Monitoring

9% SMART GLASSES
Situational Awareness, Remote Support/Assistance, Heads-up Display

4% BODY CAMERAS
Continuous Audio/Video Recording, Location Tracking, Night Recording (Infrared)

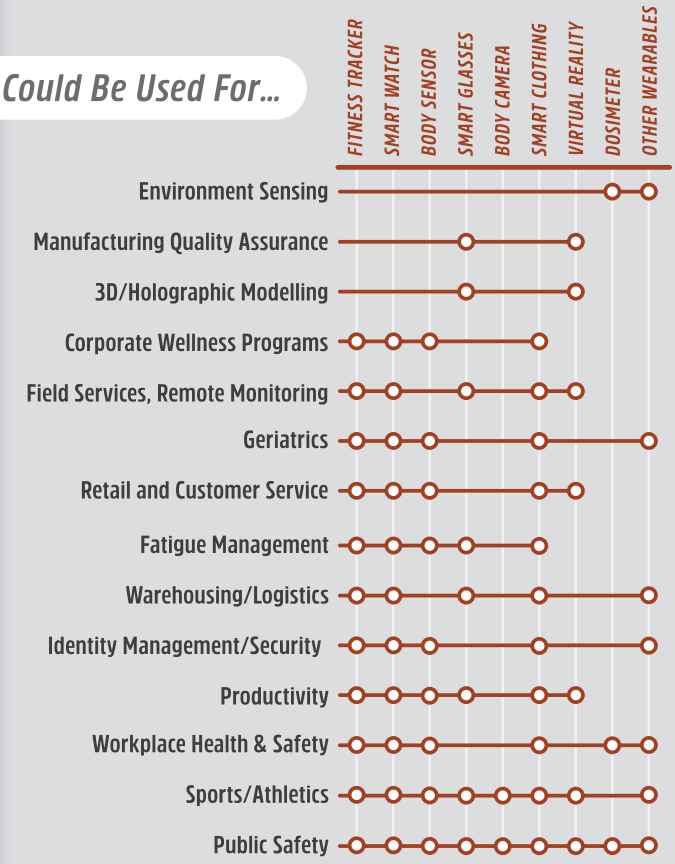
3% SMART CLOTHING & ACCS.
Athlete Coaching/Training, Activity Tracking, Driver Behaviour Monitoring

3% VIRTUAL REALITY HEADSETS
2-way Communication, Augmented Reality, Indoor Positioning/Locating

3% DOSIMETERS
Air Quality, Concussion Risk Detection, UVA/UVB (Sun Exposure)

12% OTHER WEARABLES
Biometric Authenticators, Hearables, GPS Tags, Noise Augmentation/Cancellation

Could Be Used For...



Target Workplace Markets...

30% Enterprises
Corporate Offices, Banks, Retail

29% Industrial
Oil & Gas, Mining, Manufacturing

17% Healthcare
Hospitals, Old Age Care, Rehabilitation

14% Athletics
Professional Sports, Olympic Athletes

10% Public Safety
Policing, Firefighting, Military, Security

Most Common Sensors

Of The 425 Wearable Devices...

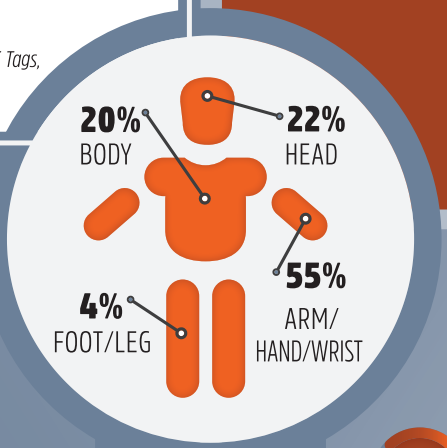
72% have an Accelerometer

29% have a Gyroscope

23% have GPS

Other Notable Sensors (<1%)

Breathing Sensor (Stretch/Non-Spirometer), Electrooculography, Eyelid Tracking (LED, Infrared), Air Quality (Particle Count/ Concentrations)



Body Location

Types of Info Measured...

- 76% Motion/Displacement
- 36% Physiological
- 30% Environmental
- 7% Social
- 2% Psychological

SURVEILLANCE STUDIES CENTRE
sscqueens.org