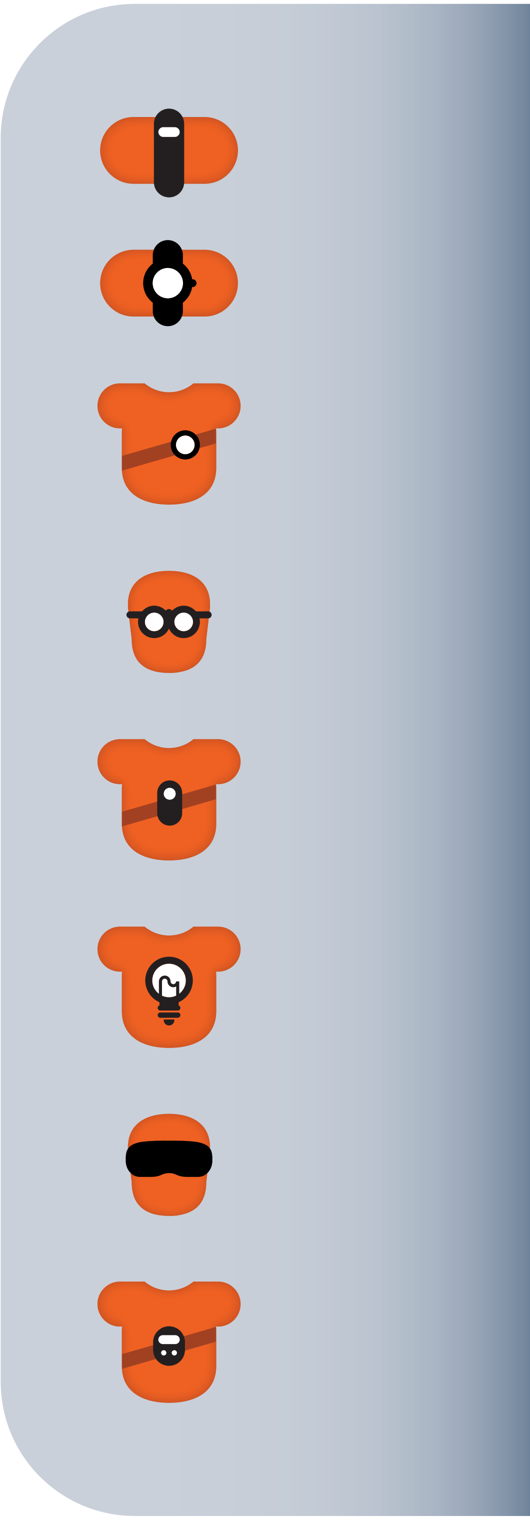
# LEFT TO THEIR OWN DEVICES?



## Privacy Implications of Wearable Technology in Canadian Workplaces

SURVEILLANCE
STUDIES CENTRE

## ABOUT THIS DOCUMENT

This project was funded by the 2016-2017 Contributions Program of the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the co-authors and do not necessarily reflect those of the OPC. As part of this program, the authors, in association with the Surveillance Studies Centre (SSC) at Queen’s University conducted an exploratory study of wearable devices in Canadian workplaces. Specifically, in an era where bodies are increasingly being represented by information, this research seeks to highlight the extent and proliferation of these devices, as well as, current information management practices and policy recommendations in the Canadian context.

## ABOUT THE SURVEILLANCE STUDIES CENTRE

The Surveillance Studies Centre is a not-for-profit multi-disciplinary research centre at Queen's University. The SSC is a leading global hub for research on expanding surveillance practices and the increasing mobility of personal data and information. Through collaborative national and international projects, the SSC examines a full range of surveillance, security, and privacy issues. We provide up-to-date analysis, seek appropriate modes of ethical assessment and democratic involvement, raise awareness with the public, and seek to inform policy at every level. Working with academic, policy and NGO partners, the SSC makes a lasting difference in organizational practices, regulatory regimes and everyday lives.

http://www.sscqueens.org

# ABOUT THE AUTHORS

**Steven Richardson:** Is a PhD Candidate in the Department of Sociology at Queen’s University in Kingston, Ontario, Canada. His research examines the development of emerging technologies in socio-technical environments – particularly, the push and pull of users' own contributions to the design and development of these technologies. Email: 14sr1@queensu.ca

**Debra Mackinnon:** Is a PhD Candidate, Department of Sociology, Queen’s University, Kingston, Ontario, Canada. Her research focuses on urban governance and the creation of Canadian public-private surveillance networks. Email: 14dmm3@queensu.ca

## Project Supervisors

**David Lyon:** Fellow of the Royal Society of Canada, Director, Surveillance Studies Centre, Professor, Department of Sociology and Faculty of Law, Queen's University

**David Murakami Wood:** Canada Research Chair Tier II in Surveillance Studies, Associate Professor, Department of Sociology, Queen’s University

## Administration and Support

**Joan Sharpe:** Project Administrator, Surveillance Studies Centre, Queen’s University

**Emily Smith:** Research Associate, Surveillance Studies Centre, Queen’s University

# RECOMMENDED CITATION

Richardson, S. and D. Mackinnon. (2017). *Left to their own Devices? Privacy Implications of Wearable Technology in Canadian Workplaces*. Surveillance Studies Centre. Available at: http://www.sscqueens.org/publications/left-to-their-own-devices

# 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...*

| | FITNESS TRACKER | SMART WATCH | BODY SENSOR | SMART GLASSES | BODY CAMERA | SMART CLOTHING | VIRTUAL REALITY | DOSIMETER | OTHER WEARABLES |
|---|---|---|---|---|---|---|---|---|---|
| Environment Sensing | | | | | | | | ○ | ○ |
| Manufacturing Quality Assurance | | | | ○ | | | ○ | | |
| 3D/Holographic Modelling | | | | ○ | | | ○ | | |
| Corporate Wellness Programs | ○ | ○ | ○ | | | ○ | | | |
| Field Services, Remote Monitoring | ○ | ○ | | ○ | | ○ | ○ | | |
| Geriatrics | ○ | ○ | ○ | | | ○ | | | ○ |
| Retail and Customer Service | ○ | ○ | ○ | | | ○ | ○ | | |
| Fatigue Management | ○ | ○ | ○ | ○ | | ○ | | | |
| Warehousing/Logistics | ○ | ○ | | ○ | | ○ | | | ○ |
| Identity Management/Security | ○ | ○ | ○ | | | ○ | | | ○ |
| Productivity | ○ | ○ | ○ | ○ | | ○ | ○ | | |
| Workplace Health & Safety | ○ | ○ | ○ | | | ○ | | ○ | ○ |
| Sports/Athletics | ○ | ○ | ○ | ○ | ○ | ○ | ○ | | ○ |
| Public Safety | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

## 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...*

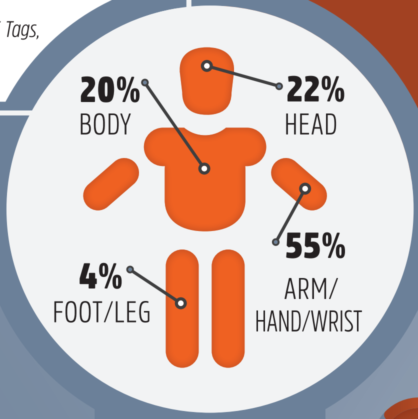
72% have an Accelerometer

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

## TABLE OF CONTENTS

# LIST OF FIGURES AND TABLES

# 1. INTRODUCTION

It has become somewhat of a truism in recent years that our devices are our biggest privacy threat. These are things that leak your information and leave marks of your quirks and routines almost by design. But this perceived privacy threat, we are told, is a necessary evil; our phones, apps, and other devices will simply not work as promised if we do not agree to service agreements setting the terms under which our personal information can be collected, used, and disclosed.

Much like current privacy laws in Canada, for the most part, these terms typically consist of exceptions – spelling out the circumstances under which information can be collected, used or disclosed without notification or consent. With few alternatives, it seems that Canadians are simply 'left to their own devices:' our stake in our data, our privacy, too readily traded in exchange for the latest 'bell' or the newest, incrementally improved 'whistle.' Privacy has been consigned to the margins; always 'catching up' with ever expanding technological (and accompanying surveillance) capabilities rarely affords the chance to 'look back' at how we've come to accept the privacy trade-off.

But, as they say, hindsight is always 20-20.

Instead, this report seeks to provide a proactive 'look forward' at a technology that is only just beginning to emerge – a technology whose issues around privacy are still being fleshed out. The name given to this latest technological trend is *wearables* – a class of devices that incorporate electronics, software, and sensors on to, on top of, and around the body. While everyday examples of wearable devices include fitness or activity trackers, smart watches and smart clothing, a surprising variety of products and applications exist and continue to be developed for use in workplaces. Ergonomic sensors for occupational health and safety, biometric sensors for professional athletes, augmented reality headsets for shipping and receiving, and smart ID badges for personnel tracking and remote monitoring are among some of the emerging trends fueling the adoption of wearable technologies in the workplace.

Current and future wearable devices have one thing in common – they render the body as information. In doing so, wearable technologies present a paradoxical situation. The more we measure and become aware about ourselves using data collected by these tracking technologies, the less control we have over how that data portrait is painted by companies that house and interpret the data, much less over who potentially has access to it. Yet at the same time as our bodies become more transparent to these monitoring devices, we become more involved with surveillance itself – participating in the collecting, analyzing, and sharing of information on ourselves.

More than just discrete measurement, wearables are designed to make users more aware of both actions being measured and the context in which they take place. Information is generated not just from every action but also from every transaction. Our bodies not only interact with information but also with 'bodies of information' (e.g., databases), leaving a trace or record of that interaction.[1]

[1] Andrejevic, M. (2007). *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, KS: University Press of Kansas., pg. 2

Recent studies have identified several non-obvious inferences that can be made about a user's behaviour and activities using action and transaction data collected from wearables. In the absence of GPS, Guha et al. discuss methods for using sophisticated algorithms to extract location and movement patterns from a device's accelerometer and gyroscope sensors.[2] This same time and space data can also be used to infer sensitive medical conditions, such as Parkinson's disease and seizures,[3] and even lead to the disclosure of psychological states, such as stress and anger.[4]

While these capabilities hint at potential ways that wearables *could* be used, in order to better evaluate current privacy concerns, more detail is needed on *how* they are being used, especially in workplace contexts. Over the coming pages, we explore the current state of wearables in the workplace, the types of devices, their capabilities and uses, in consideration of Canadian privacy laws. In doing so, we provide a number of proactive steps that decision makers, organizations, employers, employees, their representatives, and so on, can take to ensure Canadian expectations around privacy are respected.

Since most workplace wearables are directed at benefitting or improving the worker in some way – augmenting information, communication, and awareness of situations; improving efficiency, productivity, and health and safety – earning employees' trust and confidence will be of utmost importance. The path to earning that trust will be transparency and accountability in how wearables are being implemented. At this early stage, with so many isolated pilot and case studies across enterprise and industrial sectors, more work needs to be done to uncover and clarify how they are being developed, promoted, and adapted (in the case of consumer devices) to a variety of workplace contexts and use cases.

[2] Guha, S., K. Plarre, D. Lissner, D. Mitra, and B. Krishna. (2010). "AutoWitness: Locating and Tracking Stolen Property While Tolerating GPS and Radio Outages." *SenSys '10*. (November 3-5, 2010). Zurich, Switzerland. Accessed March 27, 2017 from: https://web.eecs.umich.edu/~prabal/pubs/papers/guha10autotrack.pdf

[3] Lorincz, K., B-R. Chen, G. W. Challen, A. R. Chowdhury, S. Patel, P. Bonato, and M. Welsh. (2009). "Mercury: A Wearable Senor Network Platform for High-Fidelity Motion Analysis." *SenSys '09*. (November 4-6, 2009). Berkeley, CA. Accessed March 27, 2017 from: http://projects.csail.mit.edu/wiki/pub/Evodesign/EEGSensorNetworkArchitectures/mercury-sensys09.pdf

[4] Raij, A., A. Ghosh, S. Kumar, and M. Srivastava. (2011). "Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment." *CHI 2011*. (May 7-12, 2011). Vancouver, BC. Accessed March 29, 2017 from: http://web0.cs.memphis.edu/~santosh/Papers/Privacy-CHI2011-CameraReady.pdf

# 2. BACKGROUND

## 2.1 What is a Wearable?

A surprising variety of devices are designed to follow us as we carry out our daily activities. Despite general unease toward overt surveillance and incursions into our private sphere, all of these devices measure, collect, track and transmit some aspect of that private activity, and indeed, we typically purchase them precisely for that purpose. Millions of North Americans are now accustomed to recording and sharing fitness and wellness data – everything from steps and calories to heart rate variability and sleep quality. For the most part, these devices have been limited to wrist-worn bracelets and smart watches, used primarily for everyday fitness tracking, communicating with family and friends and as tech-infused fashion. These capabilities are now literally and figuratively woven into the very fabric of our digital lives.[5] Appropriately enough, we refer to this class of devices as *wearables* – wireless and carryable devices such as clothing, apparel or accessories that are integrated with physiological or motion-based biometric sensors. Wearables have become an integral part of the Quantified Self – a movement that sees promise in quantifying, visualizing and sharing insights from a time series of self-collected data. Increasingly today, the body is represented as a machine that generates data about its various states, health, functions and activities – to be understood and portrayed via quantified calculations, predictions, and comparisons; the body/self as both subject and product of scientific measurement.[6]
The body can now be devi*ced* and devi*sed* through them.

Accordingly, one of the most difficult parts about defining 'what is a wearable' is to not only consider what form these devices take, but to distinguish these devices from others – such as mobile phones, hand-held game systems, tools or equipment. We must first ask: what is being measured or monitored – what is the capability, goal or purpose of the device?[7]

When we refer to a wearable *generally,* in this report, it refers not to the stand-alone device, but rather, to its *capacity to function as a wearable* – as a device that requires complex and interconnected systems of hard/software, data infrastructures, not to mention a host of chemical, physical, social, economic, and political arrangements. But a wearable is also more than that, it also calls forth a user.

**Wearable device**

A type of sensor, system or device whose function, application or purpose is to monitor or measure the carrying-out of action(s), whether directly or indirectly, in the context of one or many environments.

When mentioning wearables *in a particular sense,* we are referring to some type of sensor, system or device whose function, application or purpose is to measure a (psychological, physiological, environmental, social) condition, or monitor the carrying-out of action(s), whether directly or indirectly, in the context of one or many environments. To highlight these complex interdependencies when talking about wearables means that we understand it as a socio-technical

[5] Pedersen, I. (2013). *Ready to Wear: A Rhetoric of Wearable Computers and Reality-Shifting Media*. Anderson, SC: Parlor Press. See also: http://www.fabricofdigitallife.com
[6] Lupton, D. (2016). *The Quantified Self.* Malden, MA: Polity Press., pg. 98-99
[7] Starner, T. (2001). The Challenges of Wearable Computing: Part 1 & 2. *IEEE Micro*, 21(4), pg. 44

system – and likewise with personal information – it is not just personal but social, technical, and interdependent.

So, when the word 'wearable' appears it should be read with awareness of the larger picture, as the human spoke in the broader Internet of Things (IoT) ecosystem, with humans as just another node, among other 'things,' in an informational and communicational network.

## 2.2 Surveillance and Personal Information

The key advantage of wearable technologies is the ability to collect data in real-time. Although strictly speaking few devices have sensors that collect data every second, each observation is tied to a point in time when it was collected – with many abstracting from these data points to 'normalize' them overtime. In simpler terms, by plotting each observation over a normal distribution, even data points not collected can be inferred.

By providing users with constant data-enriched feedback on what they are doing, actions can be optimized towards some desired goal – be that improving lap times around a circuit, or cardiovascular performance during a full-out sprint.

At this point, clear parallels can be drawn to the decades of efforts in time management and organizational sciences to measure the optimal (or least) amount of time needed to accomplish some discrete action. But wearables are more than about achieving elite performance in competitive pursuits – primarily, they promise a *manageable means* (tied to biometric data) of improving our health, wellbeing and daily lives. It seems natural, then, to utilize these devices for the same sort of ends in the workplace.

The fact that anything that can be observed and measured on the jobsite will be tracked, reported and analysed is no doubt familiar and somewhat uncontroversial at face value. From time punch cards, to smart employee Radio Frequency Identity (RFID) cards, to GPS location tracking, driver behaviour monitoring, health and safety protective equipment, and so on, employee tracking is nothing new, but certainly not without controversy. But once the prospect of wearables tuned precisely to these use cases became a possibility, fears began to mount that employers were now going to be interested in employee heart rates, biomechanical abilities, real-time location tracking, leading to potential accidental disclosures of personal information, or at least, a loss in personal autonomy in how one accomplished their work. The gowing concern is that information from within the body, not just *about* the body, could now be used to track and monitor performance at work.

## 2.3 Key Concerns

### Reasons to Adopt

In reality however, the main prospects for utilizing wearables in the workplace are much more germane than any dystopian vision; enhancing safety and productivity in the workplace are the key concerns. Wearables carry the promise of revolutionizing occupational health and safety in Canadian mining, oil and gas, transportation and construction industries by providing detailed and targeted risk assessments, better monitoring of high-risk employees, and more effective rehabilitation of injured workers.[8]

While the means of achieving these desired goals using wearables may differ, one key difference that sets wearables apart from other Human Resource efforts is their potential to augment and boost worker's capabilities to be productive and safe. Wireless headsets and augmented reality glasses enable contextual and expert advice to be delivered directly to field services technicians, for instance, for optimized collaboration and communications. Biometric, persistent authentication methods are changing the way documents are secured and accessed. Ergonomic body sensors are aiding those with physically demanding jobs (such as construction or mining) to predict injury in advance, as well as those with desk jobs practice better posture.

Wearables in the workplace are also providing those with disabilities new opportunities for meaningful engagement. Virtual and augmented reality headsets enable those with impaired vision to interact with physical objects. Although still in their infancy, exoskeletons and bionic limbs are no longer research curiosities, having recently entered consumer and enterprise markets.

### Adoption Challenges

While there is a flood of enthusiasm regarding wearables (along with IoT) and their potential benefits in both enterprise and industrial workplaces, significant challenges remain. Although privacy and security are often discussed, the majority of wearable promoters' efforts are focused on solving industry-wide (and sometimes site-specific) technical and social/organizational challenges.

### Technical Challenges

Technical capabilities remain one of the main factors inhibiting adoption across industrial sectors who nevertheless express the most enthusiasm about adopting them. While short battery life remains an issue with lightweight, portable, data intensive devices more generally, issues related to the safety of electronic devices attached to workers, and their potential for static discharge remain a key concern in high risk workplaces such as oil & gas and mining industries. Here, any portable device must meet strict safety compliance requirements, in addition to being rugged and robust enough to usefully operate in harsh environments, such as extreme temperatures. The requirement for *intrinsically safe* electronics in hazardous environments places additional limits on devices that could be used in these scenarios. Although a device may be certified as intrinsically safe, it must also be properly employed, used, and maintained to actually be safe.

And so, while there is constant upstream pressure to design more powerful, more capable, more efficient, and safe electronics, most of the effort in deploying a wearable in a workplace is configuring and adapting the device to current needs and existing practices. Simply put, the device must *fit*. The difficulty lies not so much in finding a device most suitable for a particular use case, the difficulty is finding one that suits each individual and is congruent with the way they perform their job.

[8] Hui, S. (2015). "Wearable tech startups focus on workplace health and safety in Vancouver." Accessed March 27, 2017 from: http://www.straight.com/life/448916/wearable-tech-startups-focus-workplace-health-and-safety-vancouver

Virtual reality headsets, smart glasses and heads-up displays (HUDs) must be designed for wide variation in worker's visual capabilities. For instance, near/far-sightedness, in addition to having an adjustable nosepiece and ear stems – not just for user comfort, but also to prevent undue eye strain from focusing on a small or close-up screen display for long periods. Technical features of the device must accommodate – rather than disrupt – both worker and work; here user experience and interface design becomes paramount.

Getting users on board with new ways of interacting with information on the job (e.g., voice-based interaction, or gesture-based as opposed to the more conventional screen-based), is crucial not only for user-acceptance, but also to ensure they are capable of comprehending the data coming in and out of the device. Thus, training employees how to use the device – whether built-in as a condition of using it (e.g., user discovers and interprets device features on their own terms) or as part of tutorial session – is an important condition for obtaining consent that is informed. For this data to be useful to workers, it needs to be both informative and instructive. It needs to augment abilities but also enhance workers' capability to augment their abilities, perhaps hinting at an 'intrinsic' potential for wearables to catalyze more interest in and awareness of contemporary data flows.

Even so, there are still concerns over the security and accuracy of the data collected by wearable sensors. A previous OPC-funded project assessed the security features of popular consumer fitness trackers, and with the exception of one (Apple Watch), found most of them lacked robust security features.[9] Data security is one of the highest priorities in workplace IT systems, but having the most secure system in the world means nothing if the data isn't accurate.

In basic terms, the accuracy of the data relates to the sampling rate of the sensor combined with the method used to interpret the data (typically, sort and normalize algorithms). Sampling rate refers to the number of measurements (samples/values) made over a period of time (more technically: the process of converting an electrical signal into a numeric sequence). According to our inventory, accelerometers are the most common wearable sensor, but these can vary considerably in terms of sampling rate (ranging from 1Hz to 1kHz). A sampling rate of 1Hz means that acceleration data is collected once per second, 10Hz 10 times per second, and so on. While sampling more per second might intuitively mean a more accurate observation, it can potentially introduce unintended distortion (i.e., intermodulation), and for that matter, it depends on what is being measured (e.g., measuring brainwaves requires many samples per second, while measuring 'stairs climbed' may need only one sample per second).

Whether in the form of a torrent or trickle, this 'raw' sensor data needs to be parsed and rendered interpretable, and this is the task of the algorithm. For the most part, algorithms process data by sorting and normalizing these signals – rejecting extreme values and anomalies – comparing the resulting data plot or curve against other known models. Thus, for these algorithms to work, they need to be continually refined with more data. In a workplace scenario, this means that wearable-equipped workers are not only performing their job task (e.g., mining ore from a rock face), their work also helps improve the very algorithms used to track, quantify, and make sense of how they work. As we discuss in Section 4, due to a number of exceptions in Canadian privacy law, it is unclear if this data would be considered a 'work product' or not.

[9] Hilts, A., C. Parsons, and J. Knockel. (2016). "Every step you fake–a comparative analysis of fitness tracker privacy and security." *Open Effect Report.* Accessed March 15, 2017 from: https://openeffect.ca/reports/Every_Step_You_Fake.pdf

## Social/Organizational Challenges

Integrating new data streams into existing IT systems is typically an expensive proposition. Although many businesses we interviewed mentioned that the return on investment question was always one of the first questions clients asked during a pitch, it was always followed by concern of potential privacy issues.

Part of this unease towards workplace wearables can be traced to the growing trend of 'people analytics'[10] combined with perceptions about the biometric nature of the data collected by most wearables. On the employer side, the ability for employees to see more information about, for instance, the potential for long term injury due to exposure to physical labour may expose them to undue liability. In this case, employers express an interest in having 'not too much' ergonomic information flowing to the user, so that they do not have new grounds to sue the employer for exposing them to unsafe working conditions.

A common user perception, on the employee side, is that employers could use wearables to spy on them or monitor activities such as lunch hour or bathroom breaks. But even more than real-time location tracking, the main concern for employees is the prospect for whether aggregate data collected over a long period of time could be used to reveal behaviour patterns.[11] Privacy advocates have also warned that existing law enforcement and national security exclusions, along with Freedom of Information (FOI) requests may pose another threat to wearable-adorned employees, particularly those employed in the public sector, where FOI laws would apply.

Other organizational challenges include issues with data silos – many existing workplace technologies use proprietary systems and it is very difficult to merge or compare data across these systems. This is one of the reasons why many enterprise and industrial wearable companies are currently focused on developing interoperable platforms[12] that can merge legacy systems with newer IoT, workforce wearables, and industrial communications.

Other concerns include business process improvements (e.g., when is the right time to adopt?), implementations costs (CAPEX/OPEX), and proving ROI (return on investment). But these are merely financial issues; more significant will be socio-cultural concerns and part of this includes broader societal, workplace-specific and individual privacy concerns. In what follows, we help clarify some of these concerns by detailing the precise purposes and capabilities of currently available workplace wearables.

[10] People analytics is a method of analysis used by managers and executives to evaluate their employees or workforce. Human resource departments use people analytics for identifying talent, making hiring decisions, and assessing employee performance and retention.

[11] Starner 2001, *supra* note 7.;
Guha, S., K. Plarre, D. Lissner, D. Mitra, and B. Krishna. (2010). "AutoWitness: Locating and Tracking Stolen Property While Tolerating GPS and Radio Outages." *SenSys '10*. (November 3-5, 2010). Zurich, Switzerland. Accessed March 15, 2017 from: https://web.eecs.umich.edu/~prabal/pubs/papers/guha10autotrack.pdf
Raij, A., A. Ghosh, S. Kumar, and M. Srivastava. (2011). "Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment." *CHI 2011*. (May 7-12, 2011). Vancouver, BC. Accessed November 13, 2015 from: http://web0.cs.memphis.edu/~santosh/Papers/Privacy-CHI2011-CameraReady.pdf

[12] See for instance: http://vandrico.com/connected-worker/

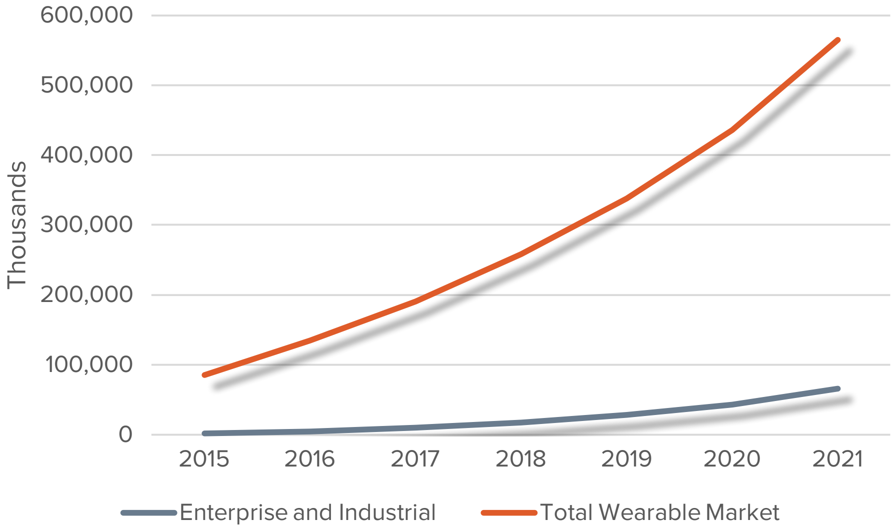
# 3. INVENTORY

This section presents the main findings of our detailed inventory of currently available workplace wearable devices. For more on how the inventory was compiled, please see Appendix A. We begin by introducing the broader market trends that have concentrated interest in certain types of wearables and certain workplace applications. We then describe the most common devices, use cases, and monitoring capabilities. This section concludes with potential ways privacy can be addressed at the device-level.

## 3.1 The Enterprise Wearable Industry

In 2015, Gartner Research announced that consumer wearables (fitness trackers and smart watches) entered the dreaded 'trough of disillusionment' of its Hype Cycle, putting them in a downward cycle of growth.[13] Since then, there has been intense interest – and market momentum – pushing for the adoption of wearables in enterprise and industrial workplace settings. Even so, enterprise and industrial wearables[14] still represent a very small portion of the overall wearable market, both in terms of total device shipments and overall revenues.[15]

Figure 1: Global Enterprise and Industrial Wearable Shipments versus Total Market, 2015-2021



*Source: Tractica 2016a*

[13] Gartner. (2016). "Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor." Accessed March 15, 2017 from: http://www.gartner.com/newsroom/id/3114217

[14] Although some studies differentiate between the two, with 'enterprise wearables' referring to those used in corporate settings and 'industrial' referring to manufacturing, outdoor/shop floor workplace environments, this report will refer to both as 'workplace wearables' and only differentiate in cases where the use case is clear that it is for corporate or non-corporate purposes.

[15] Tractica. (2016a). *Wearable Devices for Enterprise and Industrial Markets.* [2Q 2016 Research Report]. Retrieved from: https://www.tractica.com/research/wearable-devices-for-enterprise-and-industrial-markets/

The difference between wearables designed for workplace applications and wearables designed for consumer applications is that the latter includes a broad array of device types and use cases, while workplace devices are far more bespoke (i.e., configured for specific environments) and versatile – more tool-like than entertainment or fashion device. This difference is perhaps why there are many more cheaply available consumer wearables, versus their more expensive and less diverse workplace counterparts. According to our inventory, as of March 2017, out of all 425 wearables included in our study, 155 devices were designed specifically for industrial and enterprise use cases. This does not mean that the other 270 wearables we identified *are not* being used in workplaces, as discussed further below.

Bolstered by the Gartner announcement, many analysts have become concerned that interest in the consumer wearable market has plateaued, citing declining revenues and shipments.[16] Indeed, global revenues in the industrial/enterprise wearable market are expected to grow almost 2.5 times faster than the entire wearables market over the next 5 years.[17]

Another sign that attention has turned towards workplaces is that most new wearable devices announced at the Consumer Electronic Show (CES) in early 2017 were aimed at industrial/enterprise end-users. By one estimate, North American industrial/enterprise adoption of wearables will grow by 58.3% (CAGR) over the next 5 years.[18] In that same time frame, the total value (revenues) of the global industrial/enterprise market will increase from an estimated $198M (in 2015) to $12.7B (in 2021).[19]

A shown in the following figure, the main driver of growth in this segment will be enterprise wearables.

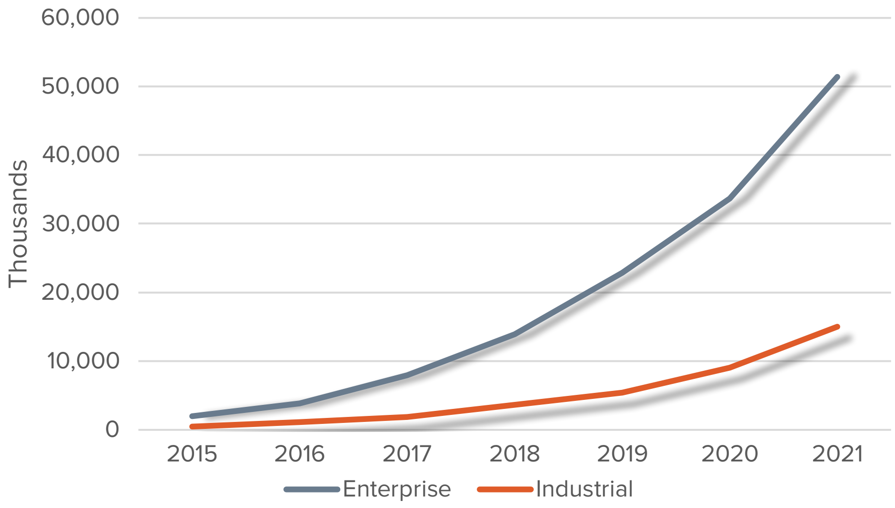
[16] IDC. (2016). "Press Release: Smartwatch Market Declines 51.6% in the Third Quarter as Platforms and Vendors Realign, IDC Finds." Accessed March 15, 2017 from: https://www.idc.com/getdoc.jsp?containerId=prUS41875116
Perez, S. (2016). "U.S. wearables market is doing much worse than expected." Accessed March 15, 2017 from: https://techcrunch.com/2016/12/21/u-s-wearable-market-is-doing-much-worse-than-expected/

[17] Tractica 2016a, *supra* note 15

[18] Ibid.

[19] Ibid.

Figure 2: Global Enterprise and Industrial Wearable Device Shipments, 2015-2021



*Source: Tractica 2016a*

These charts and figures help illustrate the broader economic trends driving investment in, and adoption of, workplace wearables.

### Canadian Market

Global investment trends have had a strong effect over the past few years on Canadian wearable entrepreneurs, start-ups and small to medium-sized businesses. Vancouver-based Recon Instruments was acquired by Intel in 2015 for $175M. In 2016, Toronto-based Pebble was acquired by FitBit for around $40M. Although these were high-profile acquisitions, the 'exit strategy' – or a company's plan to sell off assets or a stake in the business – was one of the most common discussions we had with industry stakeholders, as well as informal conversations at a number of Canadian wearable industry meetups in Toronto, Ottawa, and Montreal. According to these discussions, having an exit strategy was necessary to even entertain the interest of Series A and Series B investors. Securing these funds is necessary because developing wearable device hardware is very expensive – according to one interviewee, getting a single device, from prototype to market, can cost upwards of $30M. Once that funding is secured however, the second characteristic of Canadian wearable companies we observed was the ability to 'pivot' – or change some aspect of their business, target customer, or product.

Both characteristics – the exit strategy and the ability to pivot – point to one potential concern: given financial and market pressures to exit and/or pivot, any user data collected by Canadian wearable companies is susceptible to acquisition (i.e., disclosure) to foreign investors or multinational corporations. Although this type of disclosure is covered in Section 7.2 of PIPEDA, the contention is that Canadian companies are more likely to be acquired, and the type of personal information they might be collecting, such as user heart-beat or brain-wave signatures, may require additional protections specified in this section of PIPEDA.

The global market will remain a hotbed of interest for the years to come. Stakeholder efforts are beginning to move away from public announcements and concern with ‘hype cycles’ towards a focus on the behind the scenes work needed for wearables to be a viable option in the workplace.[20] Part of these efforts include clarifying and providing more detailed descriptions of workplace-specific device types, their capabilities, and highlighting potential workplace use cases with concrete examples.

## 3.2 Device Types (Form Factor)

Expanding upon similar databases and reports of currently available wearable devices, our inventory includes nine different device types and is current to March 2017.

Table 1: Device Types Included in the Study

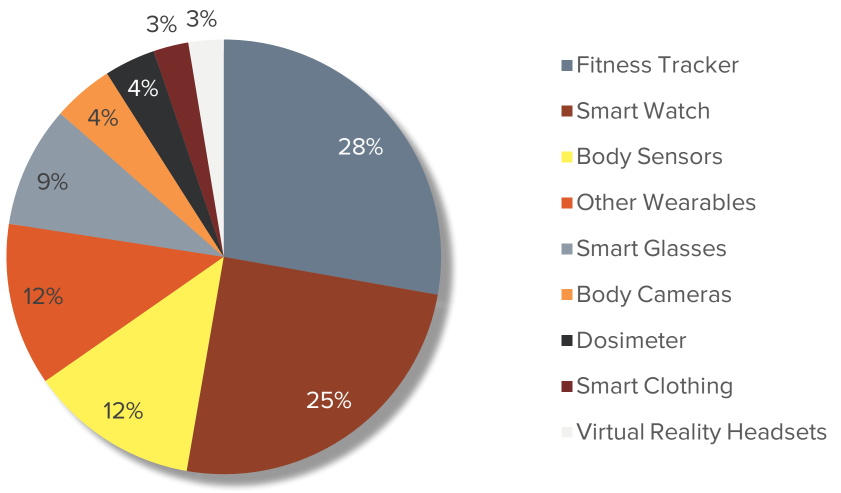
| DEVICE TYPE | DESCRIPTION |
|---|---|
| Smart Watch | Smart watches refer to devices in a wristwatch form factor that can sometimes be a stand-alone device, but more often, requires pairing with a smartphone. In most cases, smart watches extend the functionality of the smartphone as glanceable features on the wrist, such as notifications, activity and sleep tracking, payment or device authentication functions. The user can interact with the watch using touchscreens, analog 'watch-like' buttons or voice inputs. Think Apple Watch and Samsung Gear. |
| Fitness Tracker | Fitness trackers are wrist-worn and clothing clip-on devices whose core functionality is activity tracking. Compared to a smart watch, fitness trackers usually have minimal or no display. Most devices require an accompanying smartphone app in order to view activity data and statistics. Some fitness trackers also incorporate notification and coaching capabilities when paired with a smartphone. Heart rate and other physiological biometrics are also common. Think Fitbits and Misfits. |
| Smart Clothing | Smart clothing wearables are devices that take on the form factor of garments like shirts, shorts, or socks, and even includes smart accessories such as hats, jewelry, and footwear. Sensors in smart clothing take advantage of the closer fit enabled by athletic textiles, such as compression fabrics, enabling optimal location of biometric sensors. Accordingly, smart clothing devices are commonly used in sports and athletics for tracking body and muscle activity. Think Hexoskin and OMSignal. |
| Smart Glasses | Smart glasses include devices, either, designed to be worn over the eyes of the wearer, or devices designed to provide visual information to the wearer. Heads-up displays such as those used by pilots can now be incorporated into eyewear or headwear form factors. Smart glasses also include eye-tracking devices that monitor the gaze or attentiveness of the wearer, as well as augmented and mixed reality applications. Includes eyewear that is either used as a notification device connected to the smartphone, or to provide AR capabilities. Think Google Glass and Microsoft HoloLens. |
| Body Sensors | For the purposes of this study, body sensors include devices that do not measure activity like fitness trackers, but primarily measure some other physiological or psychological process. This primarily includes devices that could be used in industrial or enterprise settings: EEG headsets, wearable patches and wrist devices, such as body temperature sensors, blood pressure monitors, stress sensors; and movement sensors for ergonomics, foot pressure and gait analysis. Body sensors are primarily targeted towards professional athletes and sports teams, medical professionals and research applications. Think Interaxon Muse and Prana. |

[20] Tractica 2016a, *supra* note 15

| DEVICE TYPE | DESCRIPTION |
|---|---|
| Body Cameras | Body-worn cameras are portable audio-visual recording devices. Some devices incorporate other sensors and capabilities, such as motion and location tracking, while others have live streaming capabilities. Body cameras are used by professional athletes for first-person point of view video and by security, military and law enforcement for evidence gathering, personnel safety and accountability. Think GoPro and Taser Axon. |
| Virtual Reality Headsets | Virtual reality headsets are wearable screens that display virtual content in a virtual environment, or a digitized version of the wearer's current environment. They differ from mixed and augmented reality displays included in the 'smart glasses' category in that the primary purpose is for the wearer to explore, move about and manipulate virtual objects and environments. Think HTC Vive and Oculus Rift. |
| Dosimeter | A dosimeter is a device that measures a wearer's exposure to some external condition, force or energy. We've included concussion risk detection, vibration exposure, sun exposure, noise exposure, air quality exposure wearable devices, but excluded ionizing radiation exposure dosimeters. |
| Other Wearables | Other wearables are devices that did not fit easily into the other categories. These include Biometric authenticators, Hearables (headphones with noise cancellation/sound augmentation), GPS tags, Ring scanners, Hygiene compliance devices, Gesture-control interfaces, among many others. |

The figure below indicates the proportion of each wearable type out of all devices included in our study. Consumer wearables are included here because, in this early stage of enterprise and industrial wearable development, many companies are still using ‘off the shelf’ devices, such as smart watches for hands-free communication and notification, and fitness trackers for corporate health promotion programs. More significantly, the ‘bring your own device’ (BYOD) trend is continuing as human resource and information technology divisions within firms adjust to employees using their own wearables (BYOW) at work for accessing the Internet, answering emails, making payments, and personal activity tracking, among many other activities.

Figure 3: Proportion of all Wearables Included in Study, by Device Type



*Source: Wearable Device Inventory*

Our research indicates that smart watches and fitness trackers are the most common wearable device types currently available, lending credence to the findings in other studies that corporate wellness, notifications, and hands-free capabilities are still the main drivers of wearable adoption in the workplace.[21] The proportion of devices that are more tailored to industrial and enterprise use cases – smart glasses, body sensors and 'other wearables' – is also significant because they represent three of the fastest growing categories in this segment, year over year. Global body sensor shipments, in particular, are expected to grow by over 230% (CAGR) over the next five years.[22] These broader market trends provide an indication of which types of devices are likely to become more and more common in Canadian workplace in the coming years.

But device types and forms factors do not tell us much about privacy and surveillance concerns, they only hint at the kinds of devices, location on the body, and roughly what the potential use cases might be. Earlier in this report we defined *a wearable* as a "sensor, system or device whose function, application or purpose is to measure a (psychological, physiological, environmental, social) condition, or monitor the carrying-out of action(s), whether directly or indirectly, in the context of one or many environments." In order to better understand what these sensors are capable of monitoring, and how they render the body as information, in what follows we provide a description of all sensors uncovered in our inventory of wearable devices.

[21] Salesforce. (2015). "Putting Wearables to Work." Accessed March 15, 2017 from: https://secure2.sfdcstatic.com/assets/pdf/misc/StateOfWearablesReport.pdf
Tractica 2016a, *supra* note 15

[22] Ibid.

## 3.3 Workplace Wearable Sensors

The variety of sensors capable of being incorporated into a wearable device, though not exhaustive, helps illustrate the many ways the body – and its surroundings – are capable of being monitored, and rendered as information.

Sensoring the body also makes the wearer more accustomed to a technological form of self-monitoring – workers, now capable of being measured and understood as 'fatigued,' 'heat-stressed,' 'physically/mentally fit,' becomes not unlike the other instrumentation-equipped machines and systems they themselves may be tasked with monitoring. In both cases, the purpose of rendering the body-machine as information is to aid an actuarial logic of reducing risks in the workplace.

Table 2: Wearable Sensors and Capabilities

| SENSOR | DESCRIPTION |
|---|---|
| 3-Axis Accelerometer | An accelerometer is a device that turns movement (acceleration) of a body into digital measurements (data) when attached to the body. Most wearable devices that have an accelerometer include a compass and gyroscope, typically in a MEMS configuration known as an inertial monitoring unit (IMU), in order to measure all aspects of movement through space. |
| Air Quality Sensor (Particle count/ concentrations) | Air quality sensors are designed to monitor the concentration of pollutants in the air – with some measuring only a few, to others capable of measuring a wide-variety of harmful gases, particles, and even allergens. While most are used for outdoor environmental sensing, some are optimized for indoor settings, for instance, ensuring the airborne concentration of highly flammable wood dust at a lumber mill remains within acceptable levels. |
| Altimeter/ Barometer | Altimeters and barometers measure current altitude and air pressure, respectively. These measurements can sometimes provide a useful proxy for air temperature. |
| Blood Pressure/Rate (Piezoelectric pressure sensor) | A piezoelectric pressure sensor provides a non-invasive means to measure blood pressure by converting changes in pressure, acceleration, temperature, strain or force into electrical signals. |
| Blood Pressure/ Rate (Oscillometric sphygmomanometer) | Oscillometric blood pressure devices use an electronic pressure sensor to evaluate the oscillations of the arteries, typically in the form of a blood pressure cuff. |
| Body Temperature Sensor | Body temperature sensors use thermometers and thermistors to measure core body temperature. They are usually placed in on the torso or near arteries. |
| Breathing Sensor (Analog/ stretch-sensor) Non-Spirometer | A breathing stretch sensors uses the contractions and expansions of the wearer's chest/stomach to measure respiration. |
| Compass (3 axis Magnetometer/ Inclinometer) | A compass is a device that measures the strength and direction of magnetic fields along three perpendicular axes. |
| Camera (Visible Light) | A camera is a device that detects the spectrum of visible light using a sensor chip, most commonly (a charged-coupled device or a complementary metal-oxide semiconductor image sensor) to convert light rays into pixels |
| Camera (Infrared) | An infrared camera is a device that detects infrared radiation and converts it into an electronic signal, which is then processed to produce a thermal image and perform temperature calculations. |
| Directional Microphone | A directional microphone is a sensor that converts soundwaves emitted from a specific direction into an audio signal. |

| SENSOR | DESCRIPTION |
|---|---|
| Electrocardiogram (ECG) Sensor | The electrocardiogram sensor (ECG or EKG) is a device that records electrical and muscular functions of the heart. It can be used in combination with an Accelerometer to measure Breathing Rate. |
| Electroencephalography (EEG) | Electroencephalography (EEG) sensors are non-invasive devices which measure electrical activity in the brain. |
| Electromyography (EMG) Sensor | An electromyography (EMG) sensor is a device that monitors electrical signals generated by muscle contractions at the surface of the skin. |
| Electrooculography (EOG) Sensor | Electrooculography (EOG) is the measurement of the resting potential of the retina. Its main applications are ophthalmological diagnosis and recording eye movements. |
| Electrodermal Activity/ Galvanic Skin Response (GSR)/ Bioimpedance Sensor | Bioimpedance sensors are a set of devices which measure skin conductivity. Bioimpedance can also be used to measure respiratory rate, heart rate, and cardiovascular pressure (CVP). |
| Eyelid Tracking Sensor (e.g., LED/Infrared) | Eye tracking monitoring is used to study the visual attention of individuals. A light source (visual or infrared spectrum) is used to illuminate the cornea so that variations in eye movement can be captured as reflection patterns. |
| GPS/ GLONASS | Global Positioning System (GPS) and Global Navigation Satellite System (GLONASS) are networks of ground stations, satellites and receivers used to determine the location of receivers. |
| Gyroscope | A gyroscope is a device consisting of a mounted disk which spins about an axis in order to determine direction (angular velocity) in navigation systems. |
| Heart Rate Monitor/ Pulse Oximeter (Photoplethysmography) | A pulse oximeter is a device that indirectly monitors the oxygen saturation of blood and changes in blood volume through the skin. Most wearables that have these sensors use them only for monitoring heart rate (beats per minute) rather than blood oxygen levels, to circumvent being classified as a medical diagnostic device, which would be subject to much stricter privacy and consumer protection laws. |
| Humidity Sensor | Humidity sensors measure the concentration of water vapour in the air. Humidity control is highly crucial for a number of industrial applications, including (but not limited to): semiconductor manufacturing, food production, agriculture, pulp and paper products, gas refineries, sterilization, warehousing, and pharmaceuticals. |
| Pressure Sensor (e.g., Force sensing resistor/capacitor) | A pressure sensor is a device that typically measures resistance changes when force or pressure is applied. |
| RFID / NFC | Radio-Frequency Identification (RFID) and Near-Field Communication (NFC) are devices that use electromagnetic fields to track, identify and communicate with tagged objects. These systems consist of RFID tags, an RFID reader, and an antenna. |
| Scuba/ Snorkeling Depth Sensor | Also known as a depth gauge, these electronic sensors measure the pressure of the surrounding water in terms of PSI or bars. These sensors are crucial for underwater welding applications, for example. |
| Time-of-Flight Depth Sensor | Time-of-Flight depth sensors measure the distance to a target using a laser or other light signals and sensors. This is used for 3D object recognition, or measuring line-of-sight distance between the wearer and an object. |
| UVA/UVB Sensor (Ultra-Violet light) | UV sensors measure the intensity of incident ultra-violet radiation. Used for monitoring exposure to UVA/UVB light in environmental settings. |

These sensors collect a wide variety of information that can be broadly grouped into five categories:

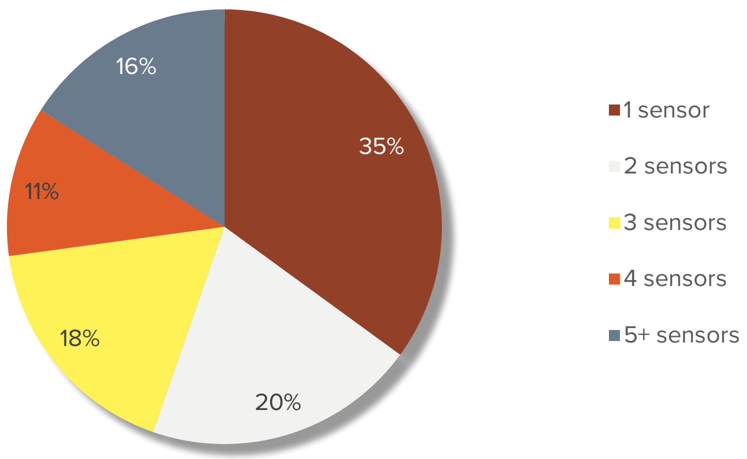
Table 3:Types of Information Measured by Wearable Sensors

| TYPE OF INFORMATION | PROPORTION |
|---|---|
| **Motion/Displacement:** Information about movement through space | 76% |
| **Physiological:** Information about body processes | 36% |
| **Environmental:** Information about external conditions/context | 30% |
| **Social:** Information about human behaviour/interactions | 7% |
| **Psychological:** Information about cognitive processes | 2% |

*Source: Wearable Device Inventory*

According to our database, the vast majority of currently available workplace wearable devices are mostly collecting motion data, such as steps, distance traveled or location.[23] Many devices also have more than one sensor, greatly enhancing the way information can be collected, combined, and communicated. For example, accelerometer data about body movements plus weight distribution and gait analysis data from a foot pressure insole can be used to estimate the onset of dementia.[24]

Figure 4: Proportion of Sensors



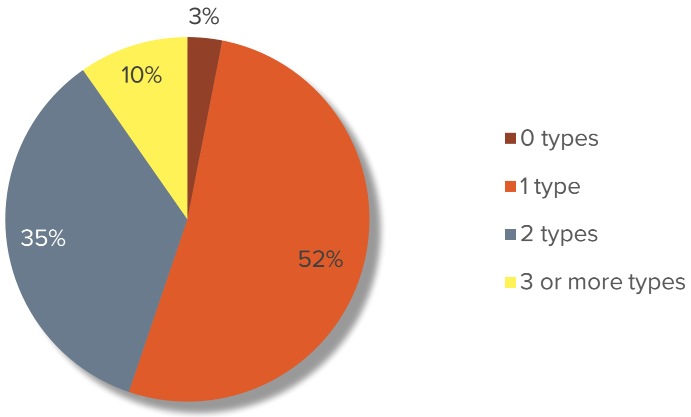
*Source: Wearable Device Inventory*

[23] Of course, this greatly oversimplifies what can be monitored via motion data. Other monitoring capabilities include, but are not limited to: concussion detection, fatigue/stress, posture, fall detection, etc.

[24] See: http://www.footlogger.com:8080/hp_new/footlogger

As we can see in the figure above, most wearables available today have more than one sensor (65%), or 2.5,[25] on average. When two or more sensors are used in conjunction, completely new monitoring capabilities and inferences are possible. For instance, a wearable equipped with an ECG heart rate sensor and an accelerometer can combine those data points to estimate breathing rate, even though it is not being measured directly, or is even measurable by each sensor alone.

Figure 5: Proportion of Devices Collecting one or more Types of Information



*Source: Wearable Device Inventory*

The figure above shows that out of all devices included in our study, most (52%) are capable of collecting only one type of information – and considering Table 3 above, for the most part, this is motion/displacement information. However, we included devices that collect 'none' of the types of information defined in Table 3 (3% in figure above) to illustrate the point that even data points not measured by sensors can be combined with sensor data to infer something about the wearer's condition or activity. All devices in general (not just wearables) are capable of collecting information based on transactional and metadata, such as time and location data or contextual information about where a device is being used (e.g., location data based on nearby Wi-Fi hotspots or known work schedules). The many possible ways sensor data can be combined (e.g., with metadata) makes it difficult to generalize the implications for privacy (see Section 3.5 for concrete examples). Information from metadata can be combined with alertness data from an EEG device to infer emotional states; devices that construct a baseline of daily living activity over the course of a week, with the help of an accelerometer, can determine eating habits such as duration and intensity.

Clearly, context matters in terms of what exactly the sensor and device in question are capable of monitoring. Based on a number of other market research reports, we found there are 14 distinct use cases for wearables, providing additional context for how sensors and the information they capable of collecting may be used in the workplace.

[25] Strictly speaking, there is no such thing as 'half a sensor'; but this average helps bridge the gap between devices that had only one sensor, and the most common wearable configuration, which was devices that had '9-axis Inertial Monitoring Units,' or IMUs, which is the typical configuration for devices that measure motion/displacement. An IMU consists of three sensors, an accelerometer, a compass, and a gyroscope.

## 3.4 Workplace Use Cases

The table below lists 14 of the most common current workplace use cases for wearable devices. The descriptions reveal the types of monitoring that are of interest for each use case, and suggest the particular ways that the body can be rendered as information.

Table 4: Major Workplace Use Cases

| WORKPLACE USE CASES | DESCRIPTION |
|---|---|
| Corporate Wellness Programs | Corporate wellness programs are a type of workplace health promotion policy designed to support healthy behaviour and improve employee health outcomes. Fitness trackers and smart watches are used in such programs to encourage a healthy lifestyle and ensure participants stay motivated. In some cases, tracking employee physical activity via steps, kilometers or calories is further incentivized by offering lower health insurance premiums – the more steps you take, the lower your risk for poor health outcomes, the lower your insurance premium. Both self-insured employers and insurance companies have started to provide wearables to employees as part of their corporate wellness programs. |
| Warehousing/ Logistics (e.g., asset management) | Wearable devices for warehousing and logistics include ring scanners for simple barcode scanning or wrist-worn computers for overlaying information about products. Voice-based headsets are also being used in warehouses to direct pickers to product locations, and for real-time training. Canada Post and DHL have already trialed a number of wearable solutions, including smart glasses, augmented reality and heads-up displays of contextual information, which have been shown to improve efficiency by almost 25%. |
| Manufacturing Quality Assurance | Automobile and aircraft manufacturers often utilize smart glasses for inspection and quality assurance. Instead of traditional inspection methods like paper-based quality assurance checks, smart glasses provide a hands-free environment for the inspector, making available more contextual information during inspection, and can even provide live video streaming to a supervisor, or a video-record of the inspection. Virtual and mixed reality headsets are also being used for computer-aided design, gesture-based computer interfaces, and even for worker point-of-view monitoring. |
| Fatigue Management | Wearables are being used to track employee fatigue and provide alerts, prevent accidents or injury across the transportation, mining, oil & gas, and aerospace industries. Example devices include fatigue monitoring hats, helmets, and headbands, as well as eye-tracking glasses. |
| Workflow/ Productivity Improvement | Wearables are being used to reduce reliance on paper-based instructions, diagrams, and other situations in which workers continually have to stop and check reference material before proceeding with their job task. They have proven useful in reducing employee errors, improving productivity, and providing much more relevant information directly to the worker more quickly than other methods. |
| 3D/Holographic Modeling for Engineering, Design, or Architectural Applications | Virtual, mixed, augmented reality headsets, and smart glasses are being used for designing myriad products, including vehicles, buildings, consumer products, and travel packages. These technologies are replacing traditional computer-aided design (CAD) software by allowing engineers to move away from 2D screen-based renderings and mock-ups to 3D holograms that can be overlaid on top of a real object. |
| Identity Management/ Security/ Authentication/Access Management | Biometric devices can use a wearer's unique heart rhythm, eye or fingerprint signature as a form of identity authentication in place of security cards, or even as two-factor token ID. The Toronto-based company Nymi is notable in this space, with its biometric wearable band being used for authentication, banking, and security in the workplace. |
| Field Services, Remote Monitoring, Training, Expert Assistance (e.g., Desk-less Professionals) | Smart glasses, smart watches, and other devices are being used by desk-less professionals (e.g., remote medicine, field technicians, etc.) to access information in the field, provide a live video feed, and for expert assistance in remote locations. Wearable cameras and smart glasses are also being used in hazardous workplaces, for instance, to provide novice technicians with access to an expert that may have health or age-related restrictions for that particular site. Live audio-visual streaming is also enabling remote monitoring and viewing capabilities. |

| WORKPLACE USE CASES | DESCRIPTION |
|---|---|
| Retail and Customer Service | Wearables are also being used to improve the retail experience and customer service of enterprises. Devices such as smart watches, smart glasses, and wearable cameras are being used in multiple ways, ranging from trialing luxury products (e.g., 'try it before you buy it' luxury cars, watches, or trips), improving customer engagement, integrating online and in-store shopping experience, and even as a marketing tool (recent examples include Disney World's MagicBand and Carnival Cruise Lines' Medallion). |
| Workplace Health & Safety | Workplace health & safety is one of the main areas of focus for industrial and enterprise wearables. Advanced alert systems, vibration and other harmful energy exposure, smart notifications, location tracking, musculoskeletal disease prevention, hygiene, and ergonomics are just some of the examples of current health and safety uses. |
| Sport/Athletics | Professional sports teams and national athletics groups are quickly turning to wearable devices to improve and monitor athlete performance, both on and off the field (e.g., sleep monitoring). Wearables are also helping coaches manage teams by optimally selecting which players are at peak performance, and even help to determine whether an injured player is ready to rejoin the team or needs more time to recover. |
| Geriatrics (e.g., Old-age care) | Wearables for old-age care are some of the earliest examples of workplace wearables. Portable blood-pressure monitors, smart pacemakers, insulin pumps, emergency assistance buttons, alert systems, and dementia patient location monitoring are common examples. These kinds of devices are being used both by healthcare facilities and by individuals to increase patient mobility, condition awareness, and rapid-access to care. |
| Public Safety (e.g., Mine rescue, First Responders, Military, Police) | Wearables for public safety applications include body temperature sensors for firefighters and mine rescue workers, body cameras for police officers, and biomechanical monitoring systems for military personnel. These devices are intended to provide biometric and audio-visual records of an event or incident, but can even be used for evaluating employee performance – in order to predict and prevent an incident. |
| Environment Sensing | Environmental sensing devices are typically used to measure the wearer's exposure to environmental hazards, such as sun exposure and chemical pollutants indoors. Humidity, temperature, air pollutants and biohazards are strictly controlled in many manufacturing and life science workplaces. Extreme work environments, such as underwater welding or deep mining involve exposure to environmental risks that can be mitigated by offering workers real-time monitoring of external conditions. |

Certain wearable devices are only practical for certain workplace use cases, providing a further means to link the types of monitoring of interest for each use case, with the way in which different wearable device types render the body as information.

Table 5: Device Type by Use Case

| DEVICE TYPE | EXAMPLE USE CASES |
|---|---|
| Smart Watches/ Fitness Tracker/ Smart Clothing | Corporate Wellness Programs |
| | Warehousing/Logistics (e.g., asset management) |
| | Fatigue Management |
| | Workflow/Productivity Improvement |
| | Identity Management/Security/Authentication/Access Management |
| | Field Services, Remote Monitoring, Training, Expert Assistance (e.g., desk-less professionals) |
| | Retail and Customer Service |
| | Workplace Health & Safety |
| | Sport/Athletics |
| | Geriatrics (e.g., old-age care) |
| | Public Safety (e.g., mine rescue, first responders, military, police) |

| DEVICE TYPE | EXAMPLE USE CASES |
|---|---|
| Smart Glasses | Warehousing/Logistics (e.g., asset management) |
| | Manufacturing Quality Assurance |
| | Fatigue Management |
| | Workflow/Productivity Improvement |
| | 3D/Holographic Modeling for Engineering, Design, or Architectural Applications |
| | Sport/Athletics |
| | Field Services, Remote Monitoring, Training, Expert Assistance (e.g., desk-less professionals) |
| | Public Safety (e.g., mine rescue, first responders, military, police) |
| Body Cameras | Sport/Athletics |
| | Public Safety (e.g., Mine rescue, First Responders, Military, Police) |
| Body Sensors | Corporate Wellness Programs |
| | Fatigue Management |
| | Workflow/Productivity Improvement |
| | Identity Management/Security/Authentication/Access Management |
| | Retail and Customer Service |
| | Workplace Health & Safety |
| | Sport/Athletics |
| | Geriatrics (e.g., old-age care) |
| | Public Safety (e.g., mine rescue, first responders, military, police) |
| Virtual Reality Headsets | Manufacturing Quality Assurance |
| | Workflow/Productivity Improvement |
| | 3D/Holographic Modeling for Engineering, Design, or Architectural Applications |
| | Field Services, Remote Monitoring, Training, Expert Assistance (e.g., desk-less professionals) |
| | Retail and Customer Service |
| | Sport/Athletics |
| | Public Safety (e.g., mine rescue, first responders, military, police) |
| Dosimeters | Environment Sensing |
| | Workplace Health & Safety |
| | Public Safety (e.g., mine rescue, first responders, military, police) |
| Other wearables | Warehousing/Logistics (e.g., asset management) |
| | Identity Management/Security/Authentication/Access Management |
| | Workplace Health & Safety |
| | Sport/Athletics |
| | Geriatrics (e.g., old-age care) |
| | Environment Sensing |
| | Public Safety (e.g., mine rescue, first responders, military, police) |

## 3.5 Example Devices

At this point it may be useful to highlight a few concrete examples of wearables that are/have been used, piloted or trialed in Canadian[26] workplaces.

### Apple Watch

| | |
|---|---|
| **Device Type** | Smart Watch |
| **Target User:** | Consumer |
| **Body Location:** | Wrist |
| **Applications:** | Activity Tracking,<br>Health and Wellness,<br>Notifications,<br>Location tracking,<br>Authentication |

| SENSORS | MONITORS |
|---|---|
| Accelerometer, Compass, Gyroscope | Motion |
| Heart Rate Monitor (Photoplethysmography) | Physiological |
| Directional Microphone | Voice |
| GPS/GLONASS | Outdoor location tracking |
| Bluetooth/RFID/NFC | Indoor location tracking |

The Apple Watch is less of a device and more of a platform for a wide variety of applications, making it one of the most versatile currently available wearables for workplace applications. A number of insurance providers in South Africa, the UK, and the United States have launched corporate wellness programs that use the device for motivation and tracking. In Nebraska, it is being used as a health care record management solution, allowing patients to receive alerts about medical appointments, new test results, billing statements, and medication reminders. Doctors can use the watch to dictate voice-based clinical notes, or even send messages to patients. It is also being used by airport staff at both London's Heathrow and Quebec City's Jean Lesage Airport for logistics and airport management, with the watch providing alerts and notifications directly on the employee's wrist.[27]

[26] Although companies rarely publicize which clients are trialing or piloting early-stage wearable devices, every attempt was made to list only those that have been used, or are very likely being used in major Canadian industrial and enterprise sectors.
[27] Tractica. (2016b). "White Paper: Enterprise Wearable Technology Case Studies." Accessed March 15, 2017 from: https://www.tractica.com/wp-content/uploads/2016/04/WP-EWCS-16-Tractica.pdf

## DAQRI Smart Helmet

| | |
|---|---|
| **Type of Device** | Smart Glasses |
| **Target User:** | Industrial/Enterprise |
| **Body Location:** | Head |
| **Applications:** | Augmented Reality, Video Streaming/Recording<br>Heads-up Display<br>Remote Expert/Technical Support<br>Situational Awareness |

| SENSORS | MONITORS |
|---|---|
| Accelerometer, Compass, Gyroscope | Motion |
| Camera (Infrared) | Environmental |
| Camera (Visible light)/Directional Microphone | Audio/visual information |
| Time of flight depth sensor | Environmental (e.g., 3D modelling, object recognition) |

The DAQRI Smart Helmet is an augmented reality personal protective equipment (PPE) device that is targeted for use in aerospace engineering, manufacturing, oil & gas, and other factory-type enterprise and industrial locations. It provides the wearer with visual information about environmental and industrial processes, including instrumentation data and thermal vision. This information can be communicated with a remote expert, who can also provide the technician with instructions and help resolve issues. By enabling first-person views, the device can be used by supervisors and managers to remotely view (and listen-in on) what the employee is currently working on. In manufacturing, shop floor workers can use the DAQRI to visualize and access control room-level data, eliminating the need to travel back and forth from the control room. Workers currently building test sites for the Hyperloop project are using the device to help novice welders operate robotic spot-welding machines. Although the company does not publicly disclose the identity of its customers, there are several North America pilot studies currently taking place and the company has been aggressively marketing the device to companies in the oil & gas extractive industries.[28]

[28] Ibid.

## OrCam MyEye

| | |
|---|---|
| **Type of Device:** | Smart Glasses |
| **Target User:** | Consumer |
| **Body Location:** | Head |
| **Applications:** | Assistive Reality |

| SENSORS | MONITORS |
|---|---|
| Camera (Visible light) | 3D Object recognition, Facial Recognition, Optical Character Recognition (OCR) |
| Directional Microphone | Voice control |

The OrCam MyEye is a smart glass device designed for users with visual impairments. It uses a forward-scanning 'smart camera' to convert visual information into spoken word. In addition to reading printed text, the device can also recognize stored faces of individuals and identify consumer products. In partnership with the Canadian Council for the Blind (CCB) and the Canadian National Institute for the Blind (CNIB), the device has been demoed across Canada. Each unit costs around $5,000 CAD, and while it is a Health Canada accredited assistive device, it is not yet subsidized by the health care system. Currently, the device is undergoing a product assessment trial with the Canadian Federal Government. The Government is considering making the OrCam available to all employees with visual impairments across all departments in Canada.[29]

[29] Cowan, P. (2016). "OrCams give the visually impaired a new view of the world." Accessed March 15, 2017 from: http://leaderpost.com/news/local-news/orcams-give-the-visually-impaired-a-new-view-of-the-world
Orcam. (2016). "OrCam Launches Assistive Tech in Canada, Establishes Toronto Headquarters." Accessed March 15, 2017 from: http://www.orcam.com/orcam-launches-assistive-tech-in-canada-establishes-toronto-headquarters/

## SmartCap

| | |
|---|---|
| **Type of Device:** | Smart Clothing |
| **Target User:** | Industrial/Enterprise |
| **Body Location:** | Head |
| **Applications:** | Driver and equipment operator alertness and fatigue |

| SENSORS | MONITORS |
|---|---|
| Electroencephalography (EEG) | Brain Activity,<br>Fatigue/Alertness levels,<br>Ability to resist sleep |

The SmartCap is a fatigue-monitoring device that attaches to a wearer's ballcap or helmet and uses brainwave (EEG) signals to measure alertness. It is used by mining, oil & gas, and transportation companies as a safety device for predicting and intervening 'microsleep events' – brief moments of fatigue-based loss of attention. According to the company's CEO, the purpose is not merely to 'detect' these events but to prevent them from occurring. Making workers more aware of their patterns of (un)alertness while on the job and educating them about the risks associated with being tired is common in the safety culture of these industries.[30] But rather than being yet another 'gauge' an operator (or their supervisor) has to monitor, the device appears to be more effective as a way to ensure workers arrive to work with enough energy to get through the day. Alertness becomes arithmetic – certain on and off-the-job factors come to be seen as enhancing or diminishing alertness while at work. The purpose of this device is to predict and prevent, not merely detect fatigue events on the job. Thus, while the device may be monitoring brain EEG levels, the employee and manager are, in effect, monitoring many factors that may have contributed to these levels inside and outside of work.

[30] SmartCap Tech. (2016). "Solutions by Industry." Accessed March 15, 2017 from: http://www.smartcaptech.com/solutions-by-industry/
Tractica. (2016b). "White Paper: Enterprise Wearable Technology Case Studies." Accessed March 15, 2017 from: https://www.tractica.com/wp-content/uploads/2016/04/WP-EWCS-16-Tractica.pdf

## Zepcam T1 Live

| | |
|---|---|
| **Type of Device:** | Body Camera |
| **Target User:** | Public Safety |
| **Body Location:** | Body |
| **Applications:** | Live Tracking, Real-time Monitoring, Situational Awareness, Live Streaming Video/Audio |

| SENSORS | MONITORS |
|---|---|
| Camera (Infrared) | Night recording |
| Camera (Visible light)/Directional Microphone | Audio/visual information |
| GPS/GLONASS | Outdoor location tracking |

The Zepcam is a body-worn camera with live streaming capabilities over Wi-Fi and cellular networks. It was specifically designed for use in public safety and industrial applications. While the device is sometimes used in industrial applications for control room-level situational awareness (i.e., locating and surveilling technicians) and remote expert assistance, body cameras are more commonly used by security and police forces for evidence gathering and personnel safety. Both the RCMP and Sûreté du Québec have piloted these devices.[31]

[31] Zepcam. (2015). "Canadian Mounties want new body-worn camera after initial testing." Accessed March 15, 2017 from: http://www.zepcam.com/news/canadian-mounties-want-new-body-worn-camera-after-initial-testing.aspx
Zepcam. (2017). "Zepcam Ti Live." Accessed March 15, 2017 from: http://www.zepcam.com/product/zepcam-t1-live.aspx

## The NYMI Band

| | |
|---|---|
| **Type of Device:** | Other Wearable |
| **Target User:** | Enterprise |
| **Body Location:** | Wrist |
| **Applications:** | Persistent Authentication |

| SENSORS | MONITORS |
|---|---|
| Accelerometer, Gyroscope | Motion |
| Electrocardiogram (ECG) Sensor | Heart Rhythm |

The Nymi Band is an authentication device that uses the wearer's electrocardiogram (ECG) or heart rhythm as a persistent form of identification. It is being used by medium and large enterprises in the financial sector, law and medicine as a secure means of accessing files and making purchases. The device also works with Apple's Fingerprint ID, enabling multifactor biometric authentication. With the Nymi, employee identification becomes a passive exercise – workers no longer have to continually recall and enter myriad login credentials, they just have to put on the bracelet and the system uses ECG to identify them and allow access. For example, if you are a nurse, perhaps you only need access to certain files to perform your job while a doctor may need access to more sensitive information. This system claims to virtually eliminate the potential for organizational privacy breaches. For instance, in cases where nurses or administrators previously may have known a physician's password and could access files for which they lacked permission, using biometric authentication tied to the wearer is intended to make this impossible. The Nymi is also notable for being one of the few wearable devices that integrates the principles of Privacy by Design – putting the user in control of their identity and securing access to their (and others') personal information.[32]

[32] Nymi. (2015). “White Paper.” Accessed March 15, 2017 from: https://nymi.com/sites/default/files/Nymi%20Whitepaper.pdf

## Humanyze GEM Badge

**Type of Device:** Other Wearable
**Target User:** Enterprise
**Body Location:** Body
**Applications:** Team Work/ Engagement, Process Optimization, Space Planning

| SENSORS | MONITORS |
|---|---|
| Accelerometer | Movement,<br>Body position |
| Bluetooth | Location tracking (iBeacons),<br>Proximity to other Badges |
| Directional Microphone | Volume, Tone,<br>Conversational dynamics |
| Infrared Sensor | Line-of-sight communication |

The Humanyze badge is a people analytics device that looks just like a typical company ID badge, but has no images or text. Instead it contains a variety of sensors that track employee relationships, behaviours, and interactions (‘sociometrics') to try and understand differences in productivity, motivation, advancement, teamwork, engagement, improve processes, and space planning. Once described as ‘a Fitbit for your career,’ the device is capable of detecting: employee location to produce heat maps of where they spend most of their time working, interacting, being productive (or not); when an employee is likely to quit; key performance indicators (KPIs) for advancement within the firm, etc. Perhaps most concerning to some is that the device uses an onboard microphone to monitor the frequency of employee conversations and how long people spend talking versus listening. It does not record the content of conversations but their occurrence; it collects metadata from the audio to feed two separate reports—one for employees and one for their managers. Combining this metadata with other information, such as email, calendars, which files they are accessing and for how long, can reveal patterns in employee productivity, motivation; it can even tell you how to improve operations or optimize space within the building. These patterns can then become visible benchmarks that other employees can use to guide their own actions, eventually, becoming a new means to interpret desirable skills, qualities and achievements. The company has piloted the device at the St. John's offices of Deloitte Canada. When interviewed about the pilot, Humanyze VP Jeremy Doyle responded that the purpose of the device is to replace existing human resource management approaches that use focus groups and employee surveys. He contends that since employees are already accustomed to self-reporting via employment review and HR surveys, they should not feel uncomfortable with the idea of a device collecting this information for them, concluding that "We're collecting the data because we can."[33]

[33] Bosanac, A. (2015). “How ‘People Analytics’ is transforming human resources.” Accessed March 15, 2017 from: http://www.canadianbusiness.com/innovation/how-people-analytics-is-transforming-human-resources/
Kane, G. C. (2015). “People analytics through super-charged ID badges.” *MIT Sloan Management Review*, 56(4)

## 3.6 Wearables and Privacy

Before addressing the broader legal and regulatory privacy landscape in Canada, it may be useful to briefly describe the organizational safeguards that should be considered when integrating wearable technologies into existing workplace systems.

- **Physical barriers.** Employers should consider ways to physically separate wearable data from potential misuse. This could include methods of ensuring that sensitive data stays on the device (i.e., not wirelessly transmitted) when in use. Once the shift ends, the device could then be stored in a secure place such as a locker or safe. It is also good practice to segregate potentially highly sensitive information from an employee's general personnel file. This would ensure such information is not accessible to administrative or accounting personnel who may have access to other personal information about the employee.
- **Technical barriers.** Access to databases where wearable data is stored from one or many devices should be secured using strong forms of encryption and authentication, such as biometric authentication (e.g., fingerprints/iris scans). These datasets should also have a records maintenance system capable of logging who accessed what files, for how long, and why they have been accessed.
- **Concealment.** Employers should consider de-identification and anonymization of wearable datasets, especially if the purpose of the device is for workplace health and safety or other forms of workforce analysis. Often these purposes can be accomplished without the need for tracking or identifying a specific individual. The wearable computer could hide sensitive information in directories with large quantities of non-sensitive information. Thus, a casual investigator could not look at all the files to determine which are the most revealing.
- **Organizational.** As with all the other measures above, the intent of these safeguards is to design ways to ensure wearable data is used only for the specified purpose for which it was produced. Accordingly, access to all wearable data should be on a 'need to know' basis; in other words, it should be limited only to those who need that information for performing their own job responsibilities. These employees should have clearly defined roles (what they can/cannot do), provisioned through appropriate training and confidentiality agreements.

Of course, the extent to which these safeguards are effective relies on many assumptions about security – that encryption or other systems cannot be reversed engineered or spoofed, that system administrators will not abuse their powers, that anonymized data cannot be re-identified, and so on. Though these risks are always present, legislative measures would provide the necessary clarity and support for these approaches to be in place prior to deploying a workplace wearable.

# 4. ASSESSMENT AND RECOMMENDATIONS

In this section, we assess the adequacy of current privacy legislation across Canada and provide recommendations for organizations, legislators and decision makers to consider when navigating worker's wearable future.

## 4.1 Types of Personal Information

In Section 3.3, we categorized the types of information capable of being collected by workplace wearable sensors according to what the sensors measure or monitor. We added the important caveat that all devices, regardless of sensor capability, can collect transactional and metadata. This makes it difficult to determine the status of these types of information in terms of existing Canadian privacy laws. Instead, we broadly consider the extent to which these types of information can be interpreted as *personal information*, *employee personal information,* or *work-product information.*

### Personal Information

Across federal and provincial substantially similar privacy laws, personal information can be simply defined as information *about* the person. The starting point for determining if a given piece of information qualifies as personal is twofold: 1) the person must be identified or identifiable – the information must relate to some element of the person's physical, genetic, geographic, mental, economic, cultural or social identity; and, 2) notwithstanding that definition and subject to any exceptions under the law, even though a piece of information may be *about* a person, it may not be considered personally identifiable – for example, anonymized or aggregated datasets. Moreover, information need not be recorded for it to be considered personal information – thus real-time data streamed to/from a wearable device could be *personal information* depending on its circumstances of use. Subject to these and other constraints, Canadian privacy laws differ significantly in terms of whether such information sourced from a wearable device, in the context of the workplace, would actually count as 'personally identifiable information.' In general, PIPEDA's definition will apply to any federally regulated organization and to commercial activities that involve interprovincial or international transactions, while substantially similar privacy laws apply to information that stays within the provincial jurisdiction.

### Employee Personal Information

Although PIPEDA gives a broad and expansive interpretation to personal information, Alberta and B.C.'s *Personal Information Protection Acts* (PIPA) helpfully distinguish between "personal information" and "employee personal information." Employee personal information is information an employer needs to manage the employment relationship; in other words, information that is *about* an individual's employment (and therefore, *excludes* any information not related to that relationship).[34]

Information related to the employment relationship would typically be anything that falls within the scope of human resources or organizational development activities. Thus wearables used for corporate wellness programs could potentially include the collection or use of employee personal

[34] Personal Information Protection Act, SA 2003, CP – 6.5., s 8(2.2) [Alberta PIPA]; Personal Information Protection Act, SBC 2003, c 63, s 8(2) [B.C. PIPA].

information – though this would likely constitute an unreasonable use of such information for that purpose. Even so, if such information is anonymized and aggregated for the purposes of workforce analysis – not to identify individual employees but to uncover trends – it would therefore not be considered 'employee personal information' and could be freely used[35] by the organization for any such purpose. A further distinction exists for information produced by an individual as a result of work-related purposes.

### Work Product Information

B.C.'s PIPA specifically excludes from the definition of personal information "information prepared or collected by an individual or group of individuals as part of the individual's or group's responsibilities or activities related to the individual's or group's employment or business, but does not include personal information about an individual who did not prepare or collected the personal information."[36] Therefore, any information that can reasonably be considered a product or outcome of work is not subject to the requirements of B.C.'s PIPA.

The test of 'reasonableness' is a common feature across all Canadian privacy statutes. The collection, use, or disclosure of any information must be reasonable, and of course, what is reasonable has varied constantly across time, space, previous decisions, and circumstances.[37] Although helpful in certain situations, this ambiguous notion makes it very challenging – for organizations, employees, and Canadians in general – to know the status of information that is produced by a wearable device in the context of work-related activities. The complainant (usually, employee, union or other representative) would have to demonstrate the unreasonableness of a particular collection, use or disclosure, while the organization (employer) would need to establish its reasonableness. Unfortunately, as existing cases show, it has been much easier to demonstrate reasonableness than unreasonableness.[38]

[35] Assuming re-identification is not possible, and assuming the purposes continue to be viewed as reasonable, given the circumstances (e.g., no other 'less invasive' reasonable alternative, etc.).

[36] B.C. PIPA, SBC 2003 c 63, s 1.

[37] Examples of inconsistencies abound: GPS data is not personal information (Otis Canada Inc. v International Union of Elevator Constructors, Local 1, [2010] B.C.C.A.A.A. No. 121); GPS data is personal information (KONE Inc., 2013 BCIPC No. 23; ThyssenKrupp Elevator (Canada) Limited, 2013 BCIPC No. 24); The "work product" of a professional is not personal information (OPC Case Summary #2001-14); The "work product" of a professional is personal information (I.M.S. du Canada Ltée. v. CAI, J.E. 2002-511).

[38] See: PIPEDA Case Summary #2003-191; PIPEDA Case Summary #2006-351; PIPEDA Case Summary #2009-001; BCIPC No. 4 University of British Columbia (Re); BCIPC No. 25 Schindler Elevator Corporation (Re).

**A Reasonable Expectation of Privacy?**

*Do employees have a reasonable expectation of privacy on employer-issued devices?*

To some extent, yes. In 2012, the Supreme Court of Canada ruled in *R v. Cole* that there is normally an expectation of privacy over one's personal records. But in an employment context, if that information is stored on an employer-owned asset and if employees were informed ahead of time of the status of that information or how it would be used (e.g., through employee contract/policy), and the employee agrees/accepts or chooses to use the device (implied consent), then they could be considered as having 'abandoned' that reasonable expectation, as long as its usage conforms to the purpose specified (and is reasonable).

*How would an employer-issued wearable compare to other corporate devices used as part of work?*

In determining if there is a reasonable expectation of privacy, a judge would consider whether the actions or practices in question are analogous or similar enough to previous actions or practices for these predecessors to be informative of reasonable expectation. If based solely on analogousness, however, a judge might compare a workplace wearable to other more commonly available consumer wearables. It would be an error of equivocation (or at least, beg the question) to generalize from one 'not overly unusual' instance of wearables, to all instances irrespective of context. What is important is whether the wearable's use *in a particular context*, *in a particular way* is 'not overly unusual' from the predecessor/precedent. The difficulty rests in selecting which similar cases constitute reasonable analogies, and which do not.

Other relevant Canadian jurisprudence that could be considered:

- **Canada:** Pacific Northwest Herb Corp. v. Thompson, 1999 CanLII 2038 (BCSC); Wansink v Telus Communications Inc., 2007 FCA 21;
- **Alberta:** Parkland Regional Library (Alberta OIPC Order F2005-003);
- **British Columbia:** Otis Canada Inc. v. International Union of Elevator Constructors, Local 1, 2010 (BCCAAA No. 21); Schindler Elevator Corporation (Order P12-01); and, Kone Inc. (Order P13-01)
- **Ontario:** Jones v. Tsige, 2012 ONCA 32.
- **Quebec:** *Université Laval* c. *Association du personnel administratif professionnel de l'Université Laval*, 2011 CanLII 6949 (QC SAT).

When considering the reasonableness of any new technology that could be used to monitor employees, courts (and arbitrators and privacy commissioners) will likely turn to previous cases examining the use of telematics and GPS devices. Telematics devices are used to collect information about workplace assets, such as vehicle usage and maintenance. Standard equipment in the transportation industry for managing fleets, these devices can also be used to monitor driver behaviour – such as speed and idle time. Although the primary purpose is to monitor vehicle health, this information can also be used to measure driver fatigue – a capability that is now being integrated with wearable technology, such as the SmartCap (see Section 3.5). Previous decisions in B.C. and Ontario[39] have determined that telematics devices do not collect personal information, while other commentators have argued that it should be considered personal information: when there is only one driver, it is very easy to connect telematics data with a particular individual.[40] Likewise with GPS tracking technologies, the Federal Commissioner has found that the loss of privacy to the employee was proportional to the benefit gained.[41]

Newly amended in 2015 by the *Digital Privacy Act*, Section 7 of PIPEDA permits the collection, use, and disclosure of personal information without consent where it was produced in the course of the individual's work or business, and the collection or use is consistent with the purposes for which it was produced. By absolving employers of the need to obtain consent for work product information, they may be emboldened to assert that employee's work product information – for example, information from smart glasses certifying an electrician performed the necessary maintenance on an aircraft wing – is therefore not subject to PIPEDA.

In summary, although 'substantially similar' on paper, in respect of matters relevant to consideration of wearables' privacy implications in the workplace, Canadian privacy laws are also substantially different. Given the requirement for employers to consider all applicable laws when assessing the potential privacy implications of their workplace activities, it is currently unclear whether information collected by a wearable (i.e., prepared/collected by an employee in context of their work) is work product information, employee personal information, or whether these distinctions are excluded by the potential for wearable data to *also* be about the individual.

But rather than wait for future complaints and case findings to clarify this issue, the one thing shared in common across Canadian privacy laws is their commitment to the 10 principles set out in Schedule 1 (Section 5) of PIPEDA. In what follows, we offer an assessment of how or whether wearables change or affect any of these principles. In doing so, our goal is to create a set of recommendations for organizations seeking to adopt wearable technologies to ensure they meet the expectations of these founding principles.

[39] Otis Canada Inc. v. International Union of Elevator Constructors, Local 82 (Telematics Devices Grievance), [2010] B.C.C.A.A.A. No. 28 (QL) (Steeves); International Union of Elevator Constructors, Local 50 v Otis Canada Inc, 2013 CanLII 3574 (ON LRB)

[40] Lacoste, S. (2010). "La surveillance des employés au travail et en dehors du travail." Accessed March 10, 2017 from: http://www.cba.org/cba/cle/PDF/adm10_lacoste_paper.pdf
Maxwell, D.L., and H. Borlack. (2014). "Telematics: Who owns the driver's data?" Accessed March 10, 2017 from: http://www.citopbroker.com/your-business/tools/is-telematics-an-invasion-of-privacy-6965

[41] PIPEDA Case Summary #2009-011

## 4.2 Assessment: Wearables and the 10 Privacy Principles

### 1. Accountablity

The principle of accountability specifies that an organization is responsible for personal information under its control. This responsibility is to be vested in an individual designated by the organization to oversee compliance – through contractual measures and the implementation of policies and practices. However, since wearables communicate the conditions and context of work on behalf of the employee, in many cases, directly and immediately to the supervisor, the giving of an account of these contexts is shifted from the employee to the device. Therefore, with wearables, some aspects of the designated individual's responsibility for overseeing compliance are downloaded to employees who may be called upon to ensure the accuracy of the information produce by the wearable, among other things.

**Recommendation:** Designate a privacy compliance officer. When considering implementing wearables in the workplace ensure personal information is handled appropriately by designating and making known an individual responsible for oversight. As with the other principles ensure staff and employees are informed about the policies and practices pertaining to how the devices will be used.

### 2. Identify the Purpose

An organization is required to notify and inform employees about the purposes of collecting personal information – specifically what it will be used for and why it is being collected. With wearables, purpose notification may shift from an active to a passive task. A smart watch for example could provide an employee with immediate notification through haptic feedback – a buzz on the wrist. But as with other forms of notification this could be quickly dismissed at a glance.

**Recommendation:** Ensure all purposes for which information collected by a wearable are documented. Provide employees with advanced notification – not just immediately before collection commences – of any new purpose through means that are not easily dismissed or ignored.

### 3. Consent

Consent is normally required to collect, use, and disclose an individual's personal information, but the purpose, nature, method, and transmission of data collected by a workplace wearable provides several exemptions to this requirement.

- **Is it personal data?** Since wearable data can be aggregated and anonymized, it may not be considered personal data.
- **Is it a work product?** Since wearable data may be produced during employment, individuals may not need to consent to its collection, use or disclosure, as long as this is consistent with the purposes specified in the notice.
- **Will it improve health and safety?** Given that many wearables are introduced to improve the health and safety of employees, in some cases this information may be considered in their best interests[42], or could be critical information that helps reduce threats to employees' health, safety and security.[43]

[42] PIPEDA, SC 2000 c 5, s7(1a).
[43] PIPEDA, SC 2000 c 5, s7(2b).

- **When wearable data is processed by a third party, is personal information being disclosed or transferred?** Outsourcing the processing of information is considered (by PIPEDA and Alberta PIPA) to be a usage or a transfer. In other words, the personal information remains under the control of the employer; it remains the responsibility of the organization and therefore would not require new consent or notice (since the third party is carrying out the purpose already specified).[44] B.C.'s PIPA and the Québec Private Sector Act, on the other hand, considers outsourcing to be a "communication" or disclosure.[45] In these jurisdictions organizations are responsible for personal information not in its custody. In general, if the third party is simply processing the employees' information on behalf of the organization and that processing is consistent with the purposes specified, then it would be considered a transfer and consent is not required. If the third party collects, uses, and/or discloses the information for any purposes of its own, it's likely to be considered a disclosure and consent would be required.

**Recommendation:** Always obtain consent. Consent and notification should include language concerning the potential for information to be transferred to a third party to ensure compliance going forward. Knowing whether information is 'transferred' or 'disclosed' is not always clear. Therefore, the purpose notification stage should inform employees that outsourcing means transferring personal information to third parties. Furthermore, the third party recipient should also consider the need to obtain consent before they receive the personal information because it is likely to be considered a commercial transaction.

However, even if consent is fully informed and the purposes are fully transparent and accountable, it still doesn't acknowledge that the data produced with wearables in the workplace is another form of work. In these cases, workers may be prevented from asserting their interests in such an economy, which would be inconsistent with the original intent of consent – informational self-determination.

### 4. Limiting Collection

In light of mass data collection and surveillance, the direct and indirect collection of personal information should be limited to the specified purpose. Similarly, the amount and type of information collected should be limited to what is reasonably necessary.

As discussed throughout this report, data can be collected directly or indirectly from the wearable device. Data can be directly provided by the sensors and subsequently live-streamed over Wi-Fi and stored in a database. This data could also be indirectly verified via another source of data. For instance, employee fatigue levels from an EEG wearable can be corroborated via a machine's telematics device broadcasting their driving behaviour.

**Recommendation:** Avoid unnecessary or indirect collection. Organizations and employers may be better off if they can limit what they have access to and see.

[44] PIPEDA, Schedule 1, art 4.1.3; Alberta PIPA s 5(2).

[45] B.C. PIPA, s 4(2); An Act respecting the Protection of Personal Information in the Private Sector, RSQ 1993, c P-39.1., s 20 [Quebec Private Sector Act].

### 5. Limiting Use, Disclosure & Retention

As mentioned under Principle 3, personal information cannot be used or disclosed without consent, except where permitted by law. Personal information should only be retained for as long as needed to accomplish the specified purpose. But again, as we've discussed above, it is unclear if data from an employer-issued wearable constitutes personal information, and therefore the extent to which employers are bound to the use, disclosure and limitation principle.

**Recommendation:** Notwithstanding this difficulty, employers should retain information sourced from a wearable for a period defined by organizational guidelines setting out retention and destruction procedures. This retention is necessary under Section 8(8) of PIPEDA requiring personal information to be retained past its destruction date in case of a future complaint.

### 6. Accuracy

Organizations should ensure that the information they are collecting and using is accurate, complete and up-to-date. It should be noted that the use of wearables in the workplace (and other big data techniques) may result in the over collection of information, a false sense of accuracy, and may increase the potential for re-identification of sensitive information that may be anonymized or aggregated in other personnel files. The sampling rates of wearable sensors may afford the opportunity to collect far too much information than is needed for the purposes specified.

Organizations may attempt to legitimize this over collection by arguing for the need to continually collect the most up-to-date information. Similarly, the rationale of this over collection may be justified under the auspices of big data to argue that data produced by wearables are more authentic, more quantifiable, and therefore, more accurate. Applying the principles of purpose limitation to such unbridled enthusiasm should work to minimize the possibility that inaccurate information will be used to make a decision about an employee. When data from a wearable is considered 'more accurate' than other reasonable means of collection, it also increases the potential for re-identification – by providing more details to be combined and connected.

**Recommendation:** 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

Information collected by a wearable must be protected against loss, corruption, modification, and theft to the extent necessary, as determined by the sensitivity of the information.

**Recommendation:** In addition to the safeguards previously outlined in Section 3.6 above, organizations should consider conducting a privacy impact assessment prior to implementing wearables in the workplace. 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

Organizations should incorporate principles of openness and transparency into guidelines, procedures, and practices (for example, BYOD and BYOW policies) that pertain to the management of information from employee's devices.

**Recommendation:** Be open about how information is managed and who is responsible. This information should be readily available, easy to understand, and accessible. A commitment to openness does not mean being open about these practices only during notice for consent; it should be posted or available in areas frequented by employees.

### 9. Access

This principle requires organizations to provide individuals access to what personal information they have about them upon request. Note however that this requirement refers to personal information; the status of information produced by a wearable remains unclear. Therefore, it is also unclear whether employees should be granted access to this data upon request. Furthermore, the variety, volume, and velocity of data produced by wearables may undermine an individual's ability to annotate, contextualize, modify, and correct errors/discrepancies in the information. For instance, it would be difficult (if not impossible) for an individual to modify an ECG documenting their heart rate variability (or heat stress) every three minutes over the course of a work shift.

Employers might also resist providing employees with all personal information they have collected given the potential to increase liability. Perhaps a heavy-duty mechanic is newly equipped with a wearable device telling them how much vibration they are being exposed to when using a tool. Would they now be open to suing the company on grounds of numerical proof of exposure to harm? The principle of access might also compromise who is responsible for the accuracy and accountability of the data produced by a wearable. Who is responsible? The wearable manufacturer? The employer-as-steward of personal information? Or the individual employee-producer of the information?

**Recommendation:** Rather than granting employees full access and modification capabilities upon request, employees' ability to access should be limited to an ability to challenge the accuracy or completeness of the information, especially when the information from a wearable is used to evaluate their performance.

### 10. Challenge Compliance

Organizations are required to designate appropriate and accountable individuals to oversee how data is handled, that the policies, practices, and procedures comply with relevant privacy legislation, and that employees have recourse to challenge that compliance.

Given all that's been discussed in this section, the difficulty of determining the applicability of information collected by a wearable device in the context of the workplace to current privacy laws in Canada, it would be unreasonable to suggest that the privacy buck stops at individual employees. Privacy is a concern shared by all stakeholders and should not only be raised in times of redress; organizations, employers, employees, decision makers, and privacy commissioners should take proactive interest in the issues that matter, not just wait for moments when the privacy trade-off becomes a privacy payoff.

**Recommendation:** 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).

# 5. CONCLUSION

Wearables promise to dramatically transform the nature of work. Occupational health and safety, productivity, and efficiency are no longer limited to incremental, post-hoc improvements but can be monitored and controlled in the same moments they take place. Workers, newly adorned with sensors, are given access to the innermost workings of their body and mind, to adjust their performance accordingly. In exchange, employers are granted the ability to more accurately pinpoint problems and more effectively manage employees. At the centre of this privacy trade-off, crucial technical, organizational, and regulatory questions remain: How are wearables protecting user data? What is the status of this information? Who is the user – the employee or the employer – and to whose privacy should we refer?

### Whose Privacy? Data Attributes & Combinations

When considering the privacy implications of wearables in the workplace, we began by understanding the broader market trends driving certain types of wearables into certain workplace use cases. This led us to consider the types of sensors being incorporated that make available and monitor different types of information about the body. The typical concern with such information is that different types of biometric data can reveal more sensitive details about the individual.

When we first started this project, we wondered whether the privacy issue of workplace wearables would be consistent with this concern over certain data attributes. In other words, could we rank the sensitivity of certain types of biometric data in advance? Intuitively, we might say *yes*; however, as we mentioned, wearables provide more than just discrete measurements. Their main purpose is to make users more aware of both the actions being measured and the context in which they take place. With the potential for metadata, we saw that information is generated not just from every action, but also from every transaction. Thus 'the privacy implications of wearables in the workplace' are not as simple as a concern with what 'kind' of data is being collected.

Combining data can yield surprising personal details that depend entirely on the interpretive context. For instance, combining accelerometer data with heart rate data, in the context of monitoring employee stress or fatigue, can be used to infer smoking, illicit drug use, or alcohol consumption; whereas in the context of a corporate wellness program, those same combinations might help determine insurance premiums in employee benefit packages. So instead of just assessing a new technology in terms of data attributes and non-obvious inferences that can be made in the aggregate, more work needs to be done distinguishing between 'what the data is produced for' versus 'what it can be used for.'

Another concern we identified was whether companies might decide to restrict data flows, or filter them, in the name of privacy. On the one hand, given the individual nature of data collected from wearables, some companies might see this as opening them up to potential liabilities. On the other hand, what if this data, anonymized and aggregated, gives the company or the device manufacturer exactly what they need to refine their algorithms? Given that most wearables in Canadian workplaces are being deployed as pilot projects, we should be careful that the 'privacy' of these datasets is not spun in a way that makes it seem like intellectual property or trade secrets. Too often we err on the side of 'the most capable stewards' of our personal data, when that very process might also strip us of access – or even a stake – in what we contribute to such competitive advantages.

### Privacy Parity?

The decision-making approach of privacy commissioners in the past has consistently sought to balance the privacy rights of individuals with the information needs of organizations. But given the number of actors with a potential stake in data produced by wearables in the course of work, how would one go about this balancing act? We believe it may be premature to evaluate wearables in the workplace in terms of discussing 'balancing' the rights and needs of one party over another, or simply evaluating reasonable trade-offs. Key questions that need to be addressed include: What will it mean if we say workplace wearable data should be considered a work product? What will it mean if we say the aggregate dataset that's at stake is the company's intellectual property? Our current regulations seem unhelpful in this regard, since personal information is, strictly speaking, limited to information *about* the person. But anonymized and aggregated data is not 'about' anyone, what matters is how it's collected and how it's used.

Furthermore, important questions about the nature of consent with wearables in the workplace remain, even though current regulation (PIPEDA) seems weak with many sections devoted to clarifying when consent *is not* required, mostly in cases when data is transferred to a third party. Considering this, the focus should be on how the data from wearables is transmitted: Is data being encrypted? Where is it being stored and for how long? Are there implicit references to principles of purpose limitation and data minimization? Does it cross provincial/national borders?

### Can Purely National Solutions Suffice?[46]

The Canadian industrial and enterprise wearable market has witnessed numerous recent high-profile acquisitions such as Pebble and Recon Jet. Under Section 7.2 of PIPEDA, when a company is acquired, all user data is transferred to the buyer and no notification or consent is needed for it to be released.

At present, the Canadian wearable device market consists mostly of start-ups, and small-medium sized businesses. For these groups the pressure to have an exit strategy is very high, which in general, suggests a tendency for wearable tech to be concentrated in the hands of a few companies. These big companies and major venture capitalist funds are all looking for the next 'killer app,' or sometimes, the next 'unicorn' that will solve the global market's decline into the 'trough of disillusionment.' Given this, it may appear that these start-ups are there mostly to take on this risk, and that early adopting companies and their employee-users are basically serving as lab rats for that investment case. The basic principle being, from the investment perspective: "if the idea fails, well, at least we have all this data."

Canada's strengths in this regard may also be its weakness: Canadian tech companies are producing cutting-edge innovations that are attractive to outside investors. If the company or intellectual property is transferred to/acquired by an outside firm, Canadian privacy law does not adequately protect the privacy interests of the company, its local employees, its clients, and customers that contributed value to that technology. The section of PIPEDA that covers this type of scenario is designed to preserve the integrity of the business transaction, not the social value of privacy that creates the competitive advantage in the first place.

[46] This question was first posed in: Bennett, C.J. and R. Grant. (1999). *Visions of Privacy: Policy Choices for the Digital Age.* Toronto: University of Toronto Press, pg. 12

Going forward, it is clear that Canada's privacy landscape should not only take an inward, national focus. We are starting to see the adoption of bilateral data sharing agreements, such as the EU-US Privacy Shield; harmonized data protection agreements, such as the GDPR; and omnibus multi-state trade agreements, such as the TPP, along with the Canada-EU Trade Agreement (CETA) coming into force later this year. Uncertainty with the current American political situation notwithstanding, it is in our best interests to ensure that Canadians do not just become the lab rats of other nations and 'approved third-parties' under these agreements who hold the legal right to take advantage of our relatively cheap and easy to acquire data.

### Privacy: A Canadian Competitive Advantage

We should not see wearables as inimical to privacy; rather, we should explore ways they can serve to complement to it. To instill greater sense of trust and confidence in the adequacy of Canada's privacy laws, much more needs to be done in making clear the social and economic value of data – not just to powerful entities capable of harnessing this value (i.e., big data analytics), but also to the individuals that produce it. The effectiveness of any system of privacy protection depends on the active and/or willful participation of those with a stake in the issue.

To foster greater awareness and engagement among Canadians in the contemporary privacy issues that matter, especially in regards to the rise of wearables in the workplace, will require "a strong, comprehensive and unambiguous law; and active and assertive regulatory authority; a strong commitment to privacy by data controllers; *a set of market incentives that drive companies to be pro-privacy and to adopt strong self-regulatory mechanisms;* a vigilant, concerned and activist citizenry and the understanding and application, at the outset of system development, of privacy-enhancing technologies."[47]

Although we have discussed some ways in which current law can improve these matters in relation to wearables in the workplace (namely, clarifying the status of information produced by wearables in the workplace, as discussed in Section 4.1), we believe the italicized line in the quote above to be a promising current competitive advantage and potential strength of Canadian privacy law. A number of our interviewees agreed that clients outside Canada and the US find PIPEDA's data localization mandate[48] attractive given these bilateral sharing agreements, along with fears over openness to US surveillance and the Patriot Act.

But more than all these issues, we should not see the emergence of wearables in the workplace only as a warning sign that our employers' main concern is with the unremitting pursuit of competitive advantage or workplace efficiency at the expense of building trust and confidence. They should be seen as a means of augmenting workers' skills and capabilities; they should be introduced equitably, and aim at levelling the playing field between all workers, regardless of ability or status. They should encourage accountability and transparency. We should not lose sight of their potential to augment, rather than further a loss of autonomy. Their potential to improve privacy in the workplace, to further promote equity, and raise the status of workers who may now have more reasonable, numerical, grounds to ask for a raise, or to argue for collective rights, these are promising avenues for us to promote.

[47] Bennett, C.J. (2008). *The Privacy Advocates: Resisting the Spread of Surveillance.* Cambridge, MA: MIT Press., pg. 222, emphasis added.
[48] i.e., cross-border restrictions in PIPEDA; although Article 14.13 of the TPP may now prohibit this.

Unfortunately, the questions raised in this last section signal important, legal questions that may only ever be addressed if a complaint is made, given the ombudsmen role of Canadian privacy commissions. But even so, Canadian workers do not have to be '*left* to their own devices,' the ever present threat of unwanted surveillance or threats to privacy need not be the only story. Canadians and businesses alike must come to terms with this new biometric medium of expression, and government must work to ensure our existing values and rights extend there as well.

# APPENDIX A: METHODOLOGY

### Primary Research

Primary research consisted of interviews and discussions with a targeted sample of Canadian industry stakeholders. We focused only on selecting those who have previously publicly commented on, or are directly involved in, the development of workplace wearables. The purpose of these interviews was to examine the extent to which issues of privacy and related regulations featured among discussions, understandings, and considerations of wearables in the workplace. To protect confidentiality, we do not reproduce direct quotes from these individuals. Interview data was used to provide context for the wearable inventory, and to provide an indication of stakeholders' familiarity with Canadian privacy law.

### Secondary Research

Secondary research consisted of extensive research of publicly-available reports, consultations, opinions research, academic articles, comparative research and benchmarking, and close-reading of legal case precedents and previous (federal and provincial) privacy commissioner findings. Over 400 documents were collected; though, only the most useful and credible ones are presented here – see Appendix B. A consulting report was also purchased from the research firm Tractica. It provides a rigorous overview of the enterprise and industrial wearable market, current case studies, and guidance for prospective adopters of workplace wearable technology solutions.

Secondary research also informed the wearable device inventory – for the purposes of describing the range of devices, capabilities, and marketed workplace purposes. It was created by combining a number of publicly-available databases

There are a number of caveats to this inventory. Due to space constraints, the scope/purpose of this report, and confidentiality issues, we are not able to provide public access to this database – please contact the authors if you require more information. Our aim for this component of the study was to provide only summary or descriptive statistics about currently available workplace wearable devices and accompanying use cases and capabilities in order to inform what types of information is capable of being collected about workers using wearables.

# APPENDIX B: WORKS CITED

### In the report: Canadian Privacy Laws, Regulations and Jurisprudence

Federal

- OPC Case Summary #2001-14
- Personal Information Protection and Electronic Documents Act, SC 2000, c 23 [PIPEDA]
- Pacific Northwest Herb Corp. v. Thompson, 1999 CanLII 2038 (BCSC)
- PIPEDA Case Summary #2003-191
- PIPEDA Case Summary #2006-351
- PIPEDA Case Summary #2009-001
- PIPEDA Case Summary #2009-011
- R v. Cole, 2012 SSC 53
- Wansink v. Telus Communications Inc., 2007 FCA 21

Alberta

- Personal Information Protection Act, SA 2003, CP – 6.5., s 8(2.2) [Alberta PIPA]
- Parkland Regional Library (Alberta OIPC Order F2005-003)

British Columbia

- Personal Information Protection Act, SBC 2003, c 63, s 8(2) [B.C. PIPA]
- *Otis Canada Inc. v. International Union of Elevator Constructors, Local 82 (Telematics Devices Grievance)*, [2010] B.C.C.A.A.A. No. 28 (QL) (Steeves)
- O*tis Canada Inc. v International Union of Elevator Constructors, Local 1*, [2010] B.C.C.A.A.A. No. 121)
- BCIPC No. 4 University of British Columbia (Re)
- KONE Inc., 2013 BCIPC No. 23
- ThyssenKrupp Elevator (Canada) Limited, 2013 BCIPC No. 24;
- BCIPC No. 25 Schindler Elevator Corporation (Re)

Ontario

- Jones v. Tsige, 2012 ONCA 32
- International Union of Elevator Constructors, Local 50 v Otis Canada Inc, 2013 CanLII 3574 (ON LRB)

Quebec

- An Act respecting the Protection of Personal Information in the Private Sector, RSQ 1993, c P-39.1., s 20 [Quebec Private Sector Act]
- I.M.S. du Canada Lteé. v. CAI, J.E. 2002-511
- Université Laval c. Association du personnel administratif professionnel de l'Université Laval, 2011 CanLII 6949 (QC SAT)

### In the report: Secondary research

- Andrejevic, M. (2007). *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, KS: University Press of Kansas., pg. 2
- Bennett, C.J. and R. Grant. (1999). *Visions of Privacy: Policy Choices for the Digital Age.* Toronto: University of Toronto Press

- Bennett, C.J. (2008). *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA: MIT Press
- Bosanac, A. (2015). “How ‘People Analytics’ is transforming human resources.” Accessed March 15, 2017 from: http://www.canadianbusiness.com/innovation/how-people-analytics-is-transforming-human-resources/
- Cowan, P. (2016). “OrCams give the visually impaired a new view of the world.” Accessed March 15, 2017 from: http://leaderpost.com/news/local-news/orcams-give-the-visually-impaired-a-new-view-of-the-world
- Gartner. (2016). “Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor.” Accessed March 15, 2017 from: http://www.gartner.com/newsroom/id/3114217
- Guha, S., K. Plarre, D. Lissner, D. Mitra, and B. Krishna. (2010). “AutoWitness: Locating and Tracking Stolen Property While Tolerating GPS and Radio Outages.” SenSys ‘10. (November 3-5, 2010). Zurich, Switzerland. Accessed March 15, 2017 from: https://web.eecs.umich.edu/~prabal/pubs/papers/guha10autotrack.pdf
- Hilts, A., C. Parsons, and J. Knockel. (2016). “Every step you fake–a comparative analysis of fitness tracker privacy and security.” Open Effect Report. Accessed March 15, 2017 from: https://openeffect.ca/reports/Every_Step_You_Fake.pdf
- Hui, S. (2015). “Wearable tech startups focus on workplace health and safety in Vancouver.” Accessed March 15, 2015 from: http://www.straight.com/life/448916/wearable-tech-startups-focus-workplace-health-and-safety-vancouver
- IDC. (2016). “Press Release: Smartwatch Market Declines 51.6% in the Third Quarter as Platforms and Vendors Realign, IDC Finds.” Accessed March 15, 2017 from: https://www.idc.com/getdoc.jsp?containerId=prUS41875116
- Kane, G. C. (2015). “People analytics through super-charged ID badges.” MIT Sloan Management Review, 56(4)
- Lacoste, S. (2010). “La surveillance des employés au travail et en dehors du travail.” Accessed March 10, 2017 from: http://www.cba.org/cba/cle/PDF/adm10_lacoste_paper.pdf
- Lorincz, K., B-R. Chen, G. W. Challen, A. R. Chowdhury, S. Patel, P. Bonato, and M. Welsh. (2009). “Mercury: A Wearable Senor Network Platform for High-Fidelity Motion Analysis.” SenSys ‘09. (November 4-6, 2009). Berkeley, CA. Accessed March 27, 2017 from: http://projects.csail.mit.edu/wiki/pub/Evodesign/EEGSensorNetworkArchitectures/mercury-sensys09.pdf
- Lupton, D. (2016). *The Quantified Self*. Malden, MA: Polity Press.
- Maxwell, D.L., and H. Borlack. (2014). “Telematics: Who owns the driver’s data?” Accessed March 10, 2017 from: http://www.citopbroker.com/your-business/tools/is-telematics-an-invasion-of-privacy-6965
- Nymi. (2015). “White Paper.” Accessed March 15, 2017 from: https://nymi.com/sites/default/files/Nymi%20Whitepaper.pdf
- Orcam. (2016). “OrCam Launches Assistive Tech In Canada, Establishes Toronto Headquarters.” Accessed March 15, 2017 from: http://www.orcam.com/orcam-launches-assistive-tech-in-canada-establishes-toronto-headquarters/
- Pedersen, I. (2013). *Ready to Wear: A Rhetoric of Wearable Computers and Reality-Shifting Media*. Anderson, SC: Parlor Press.
- Perez, S. (2016). “U.S. wearables market is doing much worse than expected.” Accessed March 15, 2017 from: https://techcrunch.com/2016/12/21/u-s-wearable-market-is-doing-much-worse-than-expected/
- Raij, A., A. Ghosh, S. Kumar, and M. Srivastava. (2011). “Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment.” CHI 2011. (May 7-12, 2011). Vancouver, BC. Accessed November 13, 2015 from: http://web0.cs.memphis.edu/~santosh/Papers/Privacy-CHI2011-CameraReady.pdf

- Salesforce. (2015). “Putting Wearables to Work.” Accessed March 15, 2017 from: https://secure2.sfdcstatic.com/assets/pdf/misc/StateOfWearablesReport.pdf
- SmartCap Tech. (2016). “Solutions by Industry.” Accessed March 15, 2017 from: http://www.smartcaptech.com/solutions-by-industry/
- Starner, T. (2001). The Challenges of Wearable Computing: Part 1 & 2. IEEE Micro, 21(4), 44-67.
- Tractica. (2016a). Wearable Devices for Enterprise and Industrial Markets. [2Q 2016 Research Report]. Retrieved from: https://www.tractica.com/research/wearable-devices-for-enterprise-and-industrial-markets/
- Tractica. (2016b). “White Paper: Enterprise Wearable Technology Case Studies.” Accessed March 15, 2017 from: https://www.tractica.com/wp-content/uploads/2016/04/WP-EWCS-16-Tractica.pdf
- Zepcam. (2015). “Canadian Mounties want new body-worn camera after initial testing.” Accessed March 15, 2017 from: http://www.zepcam.com/news/canadian-mounties-want-new-body-worn-camera-after-initial-testing.aspx
- Zepcam. (2017). “Zepcam Ti Live.” Accessed March 15, 2017 from: http://www.zepcam.com/product/zepcam-t1-live.aspx

## Other research resources:

### Best Practices

- Future of Privacy Forum. (2016). "Best Practices for Consumer Wearables & Wellness Apps & Devices." Available at: https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf
- International Working Group on Data Protection in Telecommunication. (2015). "Working Paper on Privacy and Wearable Computing Devices." Available at: https://datenschutz-berlin.de/attachments/1155/675.50.15.pdf?1448447156
- Montgomery, K. C., J. Chester, and K. Kopp. (2016). "Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection." Available at: https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf
- Wolf, C., J. Polonetsky, and K. Finch. (2015). "A Practical Privacy Paradigm for Wearables." Available at: https://fpf.org/wp-content/uploads/FPF-principles-for-wearables-Jan-2015.pdf

### White Papers

- Deloitte. (2014). "The Internet of Things Ecosystem: Unlocking the Business Value of Connected Devices." Available at: https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/internet-of-things-iot-enterprise-value-report.html
- ITAC. (2012). "The Internet of Things." http://itac.ca/wp-content/uploads/2012/09/The-Internet-of-Things-Time-for-a-National-Discourse.pdf
- Oracle and JD Edwards. (2015). "JD Edwards EnterpriseOne Wearable Technology." Available at: http://www.oracle.com/webfolder/technetwork/tutorials/jdedwards/White%20Papers/JDEE1WearablesWP.pdf
- MaRS. (2014). "Wearable Tech: Leveraging Canadian Innovation to Improve Health." Available at: https://www.marsdd.com/wp-content/uploads/2015/02/MaRSReport-WearableTech.pdf
- PwC. (2014). "The Wearable Future." Available at: https://www.pwc.com/us/en/technology/publications/assets/pwc-wearable-tech-design-oct-8th.pdf

- Springbuk. (2016). "Wearable Technology: Unlocking ROI of Workplace Wellness." Available at: https://www.springbuk.com/wearable-study/
- Technology Advice Research. (2014). "Data Monitoring and Employee Privacy." Available at: http://technologyadvice.com/resources/data-monitoring-and-employee-privacy-study/

### Privacy in the Workplace

- Wasser, L., and E. Gratton. (2017). "Privacy in the workplace, 4th Edition." Published by LexisNexis Canada. Available from: https://store.lexisnexis.ca/en/categories/shop-by-jurisdiction/promo-8/privacy-in-the-workplace-4th-edition-skusku-cad-6447/details

### Wearable Databases

- Vandrico and Deloitte. (2017). "Wearable Database." Available at: http://vandrico.com/wearables/
- www.wareable.com

### Wearables at Work

- Accenture. (2015). "Putting Wearable Displays to Work in the Enterprise." Available at: https://www.accenture.com/t20150523T040749__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_12/Accenture-Putting-Wearable-Displays-to-Work-in-the-Enterprise.pdf
- BrainXchange. (2016). "Top Challenges of Wearables in the Workplace Parts 1-9." Available at: https://brainxchange.events/category/more/challenges/
- Goh, J.P.L, (2015). "Privacy, Security, and Wearable Technology." Available at: http://www.americanbar.org/content/dam/aba/publications/landslide/2015-november-december/ABA_LAND_v008n02_privacy_security_and_wearable_technology.authcheckdam.pdf
- Mubaloo. (2015). "Wearables in Enterprise: The Potential." Available at: http://mubaloo.com/wp-content/uploads/2015/03/Wearables-in-Enterprise-The-Potential-Mubaloo.pdf
- PwC. (2016). "Wearables in the Workplace." Available at: https://www.pwc.co.za/en/assets/pdf/wearables-in-the-workplace.pdf
- Rampton, J. (2015). “Wearables in the Workplace: The Next Big Thing?” Accessed November 8, 2015 from: http://www.forbes.com/sites/johnrampton/2015/06/18/wearables-in-the-workplace-the-next-big-thing/
- Solon, O. (2015). “Wearable Technology Creeps into the Workplace.” Accessed November 8, 2015 from: http://www.bloomberg.com/news/articles/2015-08-07/wearable-technology-creeps-into-the-workplace
- Thiel, S., J. Gorham, A. Lam, and N. Boyle. (2016). "Wearables at work: Data privacy and employment law implications." Available at: https://www.dlapiper.com/en/us/insights/publications/2016/04/wearables-at-work/
- Upskill (formerly APX Labs). (2015). "The State of Enterprise Wearables." Available at: https://upskill.io/landing/wp-state-enterprise-wearables-report/
- Weston, M. (2015)."Wearable surveillance – a step too far?", *Strategic HR Review*, 14(6) pg. 214-219

### Other Suggested Reading

- Barcena, M. B., C. Wueest, and H. Lau. (2014). “How safe is your Quantified Self?: Tracking, Monitoring and Wearable Tech.” A Report by Symantec Security Response. Accessed November 25, 2015 from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf
- Belgum, K. D., and S. Chan. (2015). “Pending amendment to California data privacy law would extend protection to geophysical location and biometric data.” Accessed November 25, 2015 from: http://www.nixonpeabody.com/files/178656_Privacy%20Alert_2JUL15.pdf
- Erwin, J. (2015). ”Wearables in the Workplace.” Accessed November 8, 2015 from: http://www.cio.com/article/2978172/wearable-technology/wearables-in-the-workplace.html
- Green, C. (2015). “Wearable technology: Latest devices allow employers to track behaviour of their workers.” Accessed November 17, 2015 from: http://www.independent.co.uk/life-style/gadgets-and-tech/news/wearable-technology-latest-devices-allow-employers-to-track-behaviour-of-their-workers-10454342.html
- Hirschberg, D. L., K. Betts, P. Emanuel, and M. Caples. (2014). *Assessment of wearable sensor technologies for biosurveillance* (No. ECBC-TR-1275). ARMY EDGEWOOD CHEMICAL BIOLOGICAL CENTER APG MD RESEARCH AND TECHNOLOGY DIR.
- IDC Canada. (2015). “Canadian Wearable Device Forecast, 2015–2019.” Accessed November 13, 2015 from: http://www.idc.com/getdoc.jsp?containerId=CA3MS15
- Langheinrich, M. (2001). “Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems.” Pg. 273-291 in *UbiComp 2001: Ubiquitous Computing.* Edited by G. D. Abowd, B. Brumitt, and S. A. N. Shafer. Heidelberg, Berlin: Springer-Verlag
- Lee, L. N., S. Egelman, J. H. Lee, and D. Wagner. (2015). “Risk Perceptions for Wearable Devices.” Accessed November 8, 2015 from: http://arxiv.org/pdf/1504.05694v1.pdf
- Motti, V. G., and K. Caine. (2015). "Users’ Privacy Concerns About Wearables: impact of form factor, sensors and type of data collected." *Proceedings of the 1st Workshop on Wearable Security and Privacy*, Puerto Rico.
- Mullen, A. (2015). “Fearing the quantified life – privacy, data and wearable devices.” Accessed November 25, 2015 from: http://thenextweb.com/insider/2015/06/05/fearing-the-quantified-life-privacy-data-and-wearable-devices/
- Nielsen. (2015). “Exploring the Privacy Concerns and Priorities of Canadians.” Report for the Office of the Privacy Commissioner of Canada. Accessed November 8, 2015 from: https://www.priv.gc.ca/information/por-rop/2015/pcp-can_201503_e.pdf
- O’Connor, S. (2015). “Wearables at work: the new frontier of employee surveillance.” Accessed November 25, 2015 from: http://on.ft.com/1IB7dz1
- OECD. (2011). “Thirty Years After the OECD Privacy Guidelines.” Accessed November 13, 2015 from: http://www.oecd.org/sti/ieconomy/49710223.pdf
- Ornstein, C. (2015). “Privacy Not Included: Federal Law Lags Behind New Tech.” Accessed November 18, 2015 from: http://gizmodo.com/privacy-not-included-federal-law-lags-behind-new-tech-1743219984
- Phoenix SPI. (2014). “Final Report: 2014 Survey of Canadians on Privacy.” Report for the Office of the Privacy Commissioner of Canada. Accessed November 8, 2015 from: https://www.priv.gc.ca/information/por-rop/2015/por_2014_12_e.pdf
- Reed, D., J. Johnson, and S. David. (2011). “The Personal Network: A New Trust Model and Business Model for Personal Data.” Accessed November 26, 2015 from: http://openidentityexchange.org/wp-content/uploads/the-personal-network-whitepaper.pdf
- Shelton, M., L. Rainie, M. Madden, Pew Research Center. (2015). “Americans’ Privacy Strategies Post-Snowden.” Accessed November 8, 2015 from: http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/

- Shilton, K., J. A. Burke, D. Estrin, R. Govindan, M. Hansen, J. Kang, and M. Mun. (2009). “Designing the Personal Data Stream: Enabling Participatory Privacy in Mobile Personal Sensing.” Accessed November 26, 2015 from: http://research.cens.ucla.edu/people/estrin/resources/conferences/2009sept-Shilton-Burke-Estrin.pdf?article=1443&context=resources
- Trenholm, R. (2015). “'Sinister' and 'Orwellian': BioBeats founder warns of the dark side of wearables and biometrics.” Accessed November 25, 2015 from: http://www.cnet.com/news/sinister-and-orwellian-biobeats-founder-warns-of-the-dark-side-of-wearables-and-biometrics/
- World Economic Forum. (2012). “Rethinking Personal Data: Strengthening Trust.” Accessed November 26, 2015 from: http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf