No Reasonable Expectation
University of California Berkeley
W231 Behind the Data

Authors: Dan Ortiz, Mohan Sadashiva

“And just like any company that blissfully ignored the Internet at the turn of the century, the ones that dismiss the Internet of Things risk getting left behind.”

— Jared Newman, Technology Journalists [Marr B.]

Table of Contents

1. Introduction

We are on a collision course. The data space and physical space are on a convergent trajectory, one where our environment and experiences are tailored to our own preferences. The same physical space may not be the same from person to person. This is the promise of the Internet of Things (IoT) and its trillions of networked sensors collecting information. From this surveillance we are modeled, our data double is generated, to tailor unique services and experiences. However, this is not the only use of our double, they increase corporate profits. To some, this sounds like a technological wonderland, to others a technocratic dystopia and the key to unlocking this treasure trove of personal data are wearables.

1.1. What Are Wearables?

Wearables, or wearable technology, refers to sensors and smart devices that are worn during everyday activities. Such devices include smart watches, fitness trackers, and heart rate monitors [Düking, P.]. In many instances these smart wearable devices pair with the user's phone via an accompanying app. These apps stream data from the device(s) to the app enabling them to track the activity the user. A common example of this is the Apple Watch. The device syncs to the users phone and streams blood oxygen levels, location, and heart rate [Apple Watch Series 6] from the device to the users phone, where the Apple Health app processes the data and saves it to the users iCloud account [Apple Health Records] for analysis and prosperity. Of course, all this personal

monitoring is done under the “notify and consent” privacy model between the user and apple.

Today’s wearables are bridging the gap between our physical world and our digital world. As Eric Schmidt, former CEO of Google, said at Davos “The internet will disappear, there will be so many IP addresses from sensors all around us, that we are wearing, that we are interacting with that it will be part of your presence all the time.” [CNBC]. It’s a matter of when, not if, employers will adopt wearable technology. Today, new technologies companies are applying the wearable concept to how we work, promising companies strong return on investment (ROI) and in the process redefining the future of work. Unlike the Apple Watch, where the user can choose not to use the technology and service, employer sponsored wearables may become a condition of employment. In today's “no reasonable expectation of privacy” policies, a world may emerge where there may not be an alternative to accepting the condition.

1.2. Wearables in Industry

Tech startups, like Intellium, are developing technologies to reduce cycle time through the application of augmented reality to reduce worker compensation through real time monitoring of workers environmental conditions and alerting of hazardous conditions. Although the offerings and application varry, these startups have one thing in common, a laser focus on how smart Personal Protective Equipment (PPE) can save customers money. The key difference between personal use and a corporate mandate is individual choice. Employees may have to consent or risk losing their livelihood.

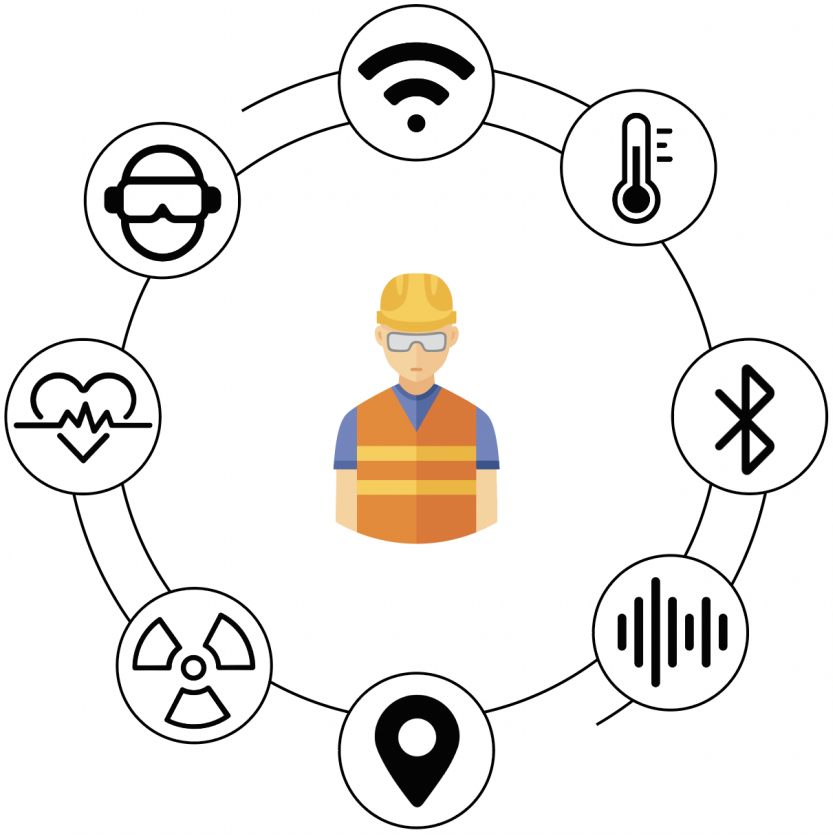
When wearable technology becomes the rule, not the exception, the future worker may not have a choice in the collection of their data.

The combination of this powerful interconnected world and company mandated wearables builds a system that is prime for abuse. However, as Sunil Paul the CEO of Sidecar put it “Convenience and ‘magic’ will overwhelm concerns. The history of technology is clear on this front…” [Marr B.]. In short, there is no putting the genie back into the bottle. Since wearable devices are poised to become part of our lives, including work, critical privacy risks must be addressed which today's “No reasonable expectation of privacy” framework is ill equipped to handle. Veronis, a security software platform company , identified it’s top five concerns with the transition to wearable technology. These include [NG]:

- Can the data collected be sold or shared to third parties
- Security and data breaches
- Is the data public or private
- Sensitive data not protected as PHI by HIPPA
- Who owns the data

To illustrate how ill equipped current corporate privacy policies are, here is what an onboarding could potentially look like in the near future.

1.3. An onboarding scenario



- Welcome to your first day on the job with ACME Construction. Our friend Tom here will demonstrate the proper use of your personal protective equipment
- Remember, you must wear your PPE at all times or you will be written up for safety violations.
- Your PPE is connected with the company network, this is to both help you perform in your job and to make sure you are safe.
- Your safety glasses are equipped with AR technology which identifies what you are working on and projects needed information over your environment, providing work instructions to schematics. You interact with the AR with simple voice commands. Remember to turn off your safety glass prior to entering the

restroom.

- For your safety, the high visibility clothing includes sensors that monitor your heart rate, body temperature and perspiration to make sure your body is not overstressing or overheating. In the event vitals are elevated, you may be asked to cool down until vitals are within acceptable range.
- In addition, your PPE includes sensors which measure the level of toxic substances and noise pollution in your vicinity. This is to ensure you are not exposed to unsafe levels while at work.
- You will be issued a company smart phone that you must use for all company communications and this needs to remain switched on with all permissions enabled during work hours. For your safety s will monitor your location and audio/video feeds as necessary. Please enable the privacy mode on the company app should you wish to temporarily suspend this function.
- You will be provided access to a company truck which will be equipped with on board diagnostics and reporting. Note that the location of the truck is monitored, and we respond to any collisions detected immediately.
- All these sensors talk to the company's servers in real time to keep you safe. Just remember, there is no reasonable expectation of privacy while using company provided devices. And remember consenting to this monitoring is a condition of employment

2. Legal considerations

To establish a reasonable expectation of privacy under current law, a person must establish two things: that the individual had a subjective expectation of privacy; and that that subjective expectation of privacy is one that society is prepared to recognize as reasonable. If either element is missing, no protected interest is established. If the individual's subjective expectation is in the context of them fulfilling their obligations as an employee, privacy protection is more complicated due to the nature of employment in the United States. Most employment is at will employment with an employment agreement. This agreement drives litigation under contract law, barring any egregious violation of employment law.

2.1. Policy

There are two opposing policy visions for regulating wearables. One policy disposition is known as the precautionary principle. Generally speaking, it refers to the belief that new innovations should be curtailed or disallowed until their developers can prove that they will not cause any harm. Advocates believe policymakers should regulate new technology quickly and address social and economic concerns preemptively.

The other policy vision is permissionless innovation. The term refers to the notion that experimentation with new technologies and business models should generally be permitted by default. Unless a compelling case can be made that a new invention will bring serious harm to individuals, innovation should be allowed to continue unabated,

and problems can be addressed later. The clash between these two visions is already evident in today's policy discussions regarding wearable and IoT technologies.

2.2. FTC

FTC looks at wearables as a natural extension of current regulations in place, including COPPA and FIPPS. However, implementing FIPPS has some practical challenges. There are practical difficulties of providing notice or and consent when certain wearables lack appropriate consumer interfaces (or simply have a small screen). FTC recommends that companies adopt a use-based model, where choice is based on the context of the interaction with the wearable [JD Supra]. Essentially the notice is given to consumers in order to allow them to make meaningful choices like setting up the device.

Similarly, the FTC recommends that data minimization can be achieved by companies tailoring their data retention needs by: choosing to collect no data; collecting data limited to the categories required to provide the service offered by the device; collecting less sensitive data; or choosing to de-identify the data collected [JD Supra]. In addition, the FTC aggressively enforces compliance often by using its broad authority under section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce.". The following are examples of recent judgments and settlements:

- Tapplock settled FTC allegations on March 20, 2020 that it deceived consumers by falsely claiming that its Internet-connected smart locks were designed to be

"unbreakable" and that it took reasonable steps to secure the data it collected from users [FTC].

- Flo Health settled Federal Trade Commission allegations on Jan 28, 2021 that the company shared the health information of users with outside data analytics providers after promising that such information would be kept private [FTC].
- DLink settled FTC allegations of lack of security of IOT communications with its home products and agreed to implement a comprehensive IOT security framework [FTC].

In addition, FTC enforcement actions can bind a company to lengthy, twenty-year privacy audits and open it up to potential liability of up to $16,000 per customer harmed per violation. Moreover, firms take a reputation hit with the press and the general public when such enforcement actions are handed down.

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have now enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information. However navigating individual state laws is a lot of overhead and fraught with conflicts. A national data breach notification law and a baseline consumer privacy statute would help clarify and solve many of the issues with privacy in the context of wearable technology.

2.3. HIPAA

HIPAA is the Health Insurance Portability and Accountability Act, which was passed in 1996 to standardize the electronic transmission of healthcare information.

This includes all forms of patient information as well as transaction data such as insurance claim data. The HIPAA privacy and security rules [Marbury] address set the standards for using, disclosing, and protecting PHI (Personal Health Information). These rules also address the rights that individuals have to understand and control how their PHI is used while simultaneously supporting the flow of health information that is needed to deliver high-quality healthcare. Similarly, HIPAA's security rules set the standards for storing and securing patient data. They require relevant entities to put physical and electronic safeguards in place that ensure PHI can be safely transmitted, received, and stored, and that it is accessible only by authorized individuals or entities [Kajeet IoT]. HIPAA defines PHI as all personally identifying health data.

Current HIPAA rules [Kajeet] do not require manufacturers of health wearables to comply with HIPAA's privacy and security laws unless the data in question is being shared with a healthcare entity (a business, professional, or services provider) that is required to comply with those rules.

2.4. HITECH

President Barack Obama signed the Health Information Technology for Economic and Clinical Health Act (the HITECH Act) in 2009 to stimulate the adoption of electronic health records and their supporting technologies to improve patient outcomes and streamline healthcare services using technology. Broadly speaking, HITECH requires [Kajeet] that all technologies and standards that apply to healthcare do not compromise HIPAA privacy and security laws and that healthcare organizations, as well as relevant businesses and service providers, be held responsible for upholding HIPAA laws and

disclosing breaches. Under HITECH, a person, company, service provider, healthcare facility, or health plan entity – including anyone working for or on their behalf – can be liable for breaching HIPAA rules. Mistakes as seemingly insignificant as improperly using PHI, not securing PHI, or giving access to unauthorized users or recipients of PHI data constitute a breach of HIPAA security and privacy laws.

2.5. IOT Improvement Act

HITECH was a precursor to the Internet of Things Improvement Act (proposed in March 2019, passed in December 2020). This act requires IoT devices [Kajeet] that are purchased by the US government to meet certain security standards. As the number of IoT devices in use grows, so do concerns about the security risks they pose. The IoT Improvement Act aims to ensure that there is a baseline for security that IoT devices of any kind must meet before they can be connected to a government network.

2.6. Contract law

To the extent that wearable technologies are used by individuals to record and gather video, audio, and other data, First Amendment rights may be implicated. There has long existed a tension between privacy and free speech rights, which will be greatly exacerbated by the rise of wearable technologies.

Wearables are used to monitor employee performance (e.g. amazon) for productivity and environmental factors to keep employees safe. Both provide real value and constitute legitimate business use in specific applications. However the absence of guard rails and frequent transgressions give an impression of overreach. Contract law

can also act as a powerful deterrent to the misuse of IoT and wearable technologies, not only in the workplace, but in many other formal relationships.

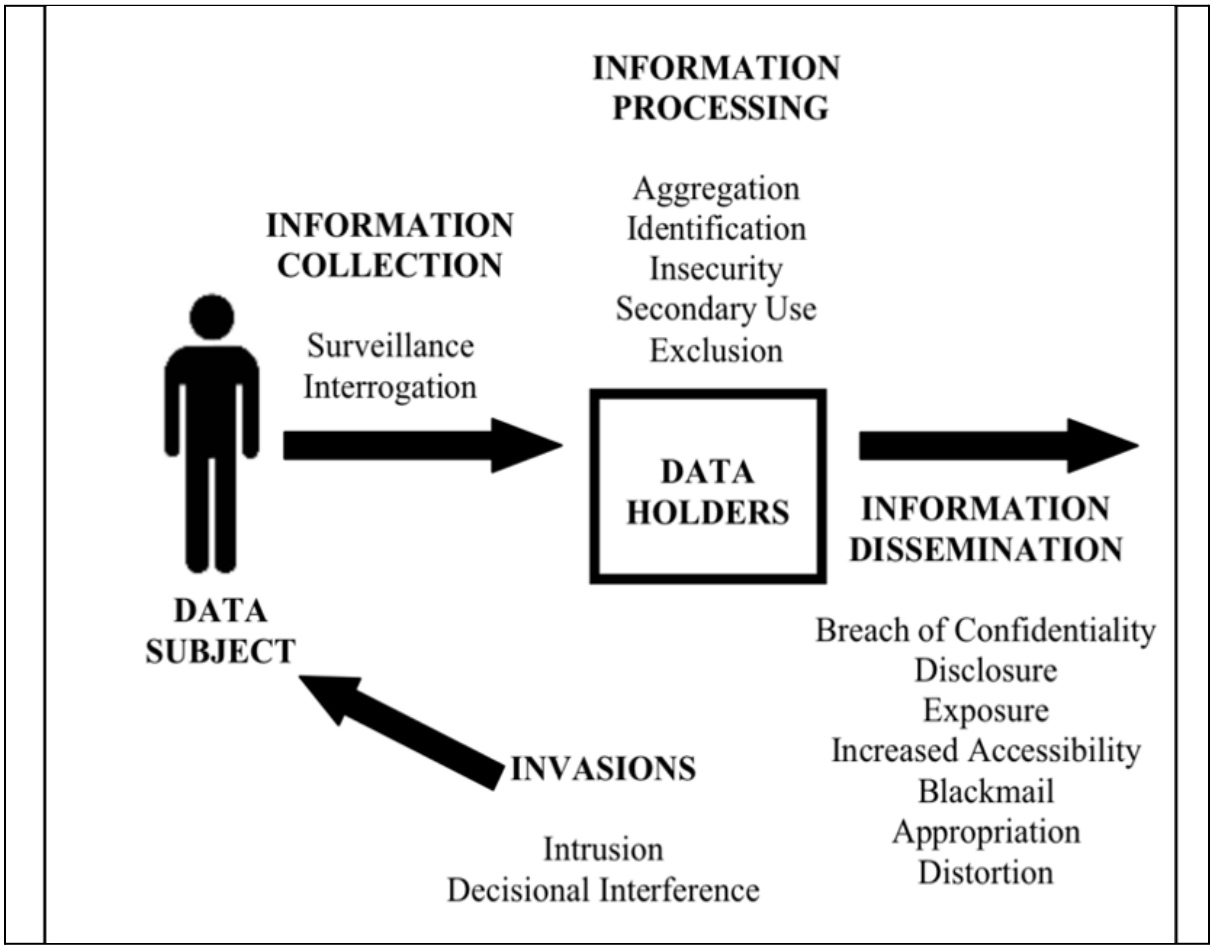
In the case of employees, the courts have consistently ruled that employees have no legitimate expectation of privacy in the content of their Internet communications made using company owned internet infrastructure and information systems. This is especially true in the case of government employees as noted by the US Supreme court in *United States v. Angevine*[11] and *United States v. Thorn.*[12].

2.7. Other laws

Other federal and state laws already exist that could address privacy concerns. Property law already addresses trespass, and court rulings have seen property norms extended to cover new types of harms involving wearable technologies. State Peeping Tom laws that prohibit peering into individual homes or even surreptitious spying in public also exist. The Video Voyeurism Prevention Act imposes fines and even jail time on those who have an “intent to capture an image of a private area of an individual without their consent, and knowingly does so under circumstances in which the individual has a reasonable expectation of privacy.” The Fair Credit Reporting Act also already offers consumers access and correction remedies for their credit records, and its provisions may apply to some of the records created through new IoT technologies.

3. Ethical considerations

3.1. Solove's Taxonomy



Information collection: It is questionable whether there is sufficient informed consent during onboarding of new employees. There are a large number of devices involved such as smartphones, tablets, computers, AR/VR headsets, wearables and each has a large number of sensors that capture data such as location, audio and video. Do the employees know all the information they are consenting to share and how this will be used?

Information processing: In any company the goals are in a constant state of evolution. For example, the company may have started monitoring location to help with dispatch and dynamic scheduling - a legitimate business use. However sometime later a data scientist discovers a correlation between the fitness bias and productivity. Does the employee know that their data is being used in such a way? Is it fair? Often employees have to provide broad based consent to the company as a condition of employment with no alternative.

Information dissemination: Most companies do not have clear disclosures and policies on who can access this data from employees. There is also no guarantee that this data is not disclosed to third parties and where that leads. For example, the company can sell the collected information to insurance companies (as secondary use) for reduced premiums, or others who then can aggregate and repurpose it.

Invasion: There are unintended consequences of collecting and processing data that could amount to an invasion of privacy. For example, using the sensors in the wearables if the company discovers that the employee has a serious disease that they are unaware of then there is no clear guideline on how they choose to proceed. Similarly a person's location can be used to track associations for purposes such as union busting and lead to targeted terminations.

3.2. Nissenbaum’s Contextual Integrity

Employee data that is collected for a specific purpose such a dispatch can get used for other purposes such as fitness levels or to map associations. This violates Nissenbaum’s principle as the data is used for purposes outside of the original context [Nissenbaum]. The US legal system tends to adopt the viewpoint of “With an express privacy policy, an employee’s ‘expectation of privacy’ is avoided” [harvard]. This is where a conflict begins to emerge between the legal definition and modern privacy frameworks. There are many secondary uses from data collected from smart personal protective equipment which can boost efficiencies. However, that same data could be used to develop social maps and insights into employees' health. It is this line, when the company stops researching its operations and starts researching its employees, that contextual integrity is violated.

3.3. Mulligan/Koopman Analytic

Where Nissenbaum’s Contextual Integrity explores the when an invasion of privacy occurs, Mulligan and Koopman’s Analytic explores the dimensions of harm. [Mulligan]

Dimensions of Theory

The dimension of theory grapples with is the privacy for, what should not be private, and why should it be private. In the realm of smart PPE, the data is a double edge sword. As discussed, the same data that can be used to benefit the company can be used to gain unprecedented insights into employees. For

example, location data can be used to track the efficiency of a companies production or distribution system but the same data can be used to build social networking maps of individuals in the company. The same data that can be used to drive efficiencies is the same data that can be used to identify and target groups of employees during a union drive.

Dimensions of Protection

Dimension of protection contends with what, exactly, is being protected and who is it protecting. In the realm of smart PPE, this is about drawing a line on what is and what is not an appropriate use of the employees collected data.

Dimensions of Harm

Dimension of harm grapples with what act violated privacy, who violated it, and who was violated. In the realm of smart PPE the act of violating privacy goes back to Solove's taxonomy in the information processing meta-harm. The violators could be the corporation, or rogue agents of the corporation who are misusing the data of the data subject.

Dimensions of Provision

Dimension of provision deals with what mechanism secures privacy and who is responsible for it. In the realm of smart PPE, there are many potential mechanisms that provide security for the data. A few of these include designing privacy into the data structure, restricting and monitoring access,

Dimensions of Scope

Dimension of scope grapples with where, how long, and scope. In the realm of smart PPE, this refers to where privacy should apply, and not apply, how long the data should be retained. For example, companies may choose to not record data when an employee is in the restroom or is in the break room if it is determined the data generated would not be value-added to the company.

4. Conclusions

4.1. Recommendations

Privacy By Design(IAAP)

Privacy by design encompasses seven principles around the data subject. The principles encompass designing privacy into the system while it is being designed instead of as an afterthought [Deloitte]. It requires the system and the designers to default to privacy at the design level keeping a user centric approach. This includes transparency, encryption, and a proactive approach to data privacy and security. Privacy is quickly becoming mandatory as seen by the number of lawsuits and the monetary impact at home and abroad. Recently, Facebook settled a $650 million dollar lawsuit due to privacy violations in the state of Illinois [AP NEWS] alone and is still managing the fall out of Cambridge Analytica. A failure to protect users' privacy carries potentially heavy liability.

For corporations implementing wearable technology for their work force it is strongly recommended to mandate privacy from the project conception, especially when working with third parties. Both the design and development team and the corporation are responsible for protecting employee data and may face severe financial and reputable damages if that responsibility is neglected.

Recommendations for privacy by design:

- Obtain informed consent on setup and subsequently through training
- Establish proper use guidelines
- Transparency - give employees more and better information about their wearables
- Data minimization - do not collect and delete any data that is not being used
- On going security notices
- Apply encryption for both data at rest and in motion

Controls

Controls, both engineered and administrative are critical to implementing privacy by design. Engineered controls include assessing what data is worth collecting and how the database is structured. To limit the potential misuse of the data, the architects may choose to separate PII into multiple independent databases and anonymize the collected data. Another potential solution is to hide the raw data from business users and only return aggregated results based on the users query.

Administrative controls often complement engineered controls. Key administrative controls include; limiting access to sensitive data to only those who

absolutely need it, logging user access and queries to the data source, auditing access to validate it is still required, and building a culture around data ethics. Building this culture around data ethics for an increasingly data driven business is critical in the long term sustainment of controls. As….[O'Reilly 167] "...social controls target a wide range of behaviors….The punishment for failing to adhere to norms may be exclusion….". This means culture can either drive organizations to or away from an ethical use of data.

A New Kind of Privacy Policy (User Agreement and Corporate Data Policy)

By now, it should be self-evident that the blanket "no reasonable expectation of privacy" policy is not adequately equipped to protect either the employee or the employer. Organizations should develop policies pertaining to what data is permissible to collect, what data is permissible to be shared with third parties, how data should be stored, and how the data should be accessed. The intent of these policies are to orient the organization on how to handle data. This is especially important as many projects are initiated outside of the traditional Enterprise / Information Technology swim lane.

In addition to corporate policies, we recommend developing independent privacy policies around each wearable deployed. Think of these like a Material Data Safety Sheet, but instead of disclosing chemical information, they should disclose what data is being collected and the legitimate business need for it, the duration the data will be held, what data is being shared outside the company and why, and how to correct bad data. Legislation like GDPR and CalOPPA can serve as guides in this venture. While the topic of consent is challenging when the use of the technology is a condition of employment, corporations should embrace transparency.

In short, today's “no reasonable expectation of privacy” is not equipped to handle the complexities wearable technology brings to the workplace. As a result, enterprises seeking to implement these technologies should do so with intent and with privacy as the default. Enterprises which choose a haphazard approach to implementing wearables risks serious financial and reputational risks if/when user privacy has been violated. Those enterprises who harness the power of wearable technology with respect to people and who foster a culture of data ethics will gain valuable insights into their operations. Those enterprises should redefine their employee privacy policies and internal data collection policies to increase data collection transparency and reduce potential harm.

4.2. Future Research

Although outside the scope of this study, there are new developments being forged all the time. One up and coming area is with ingestibles. One example is a pillcam which is a capsule the size of a large vitamin that travels through a patient’s digestive system over the course of several hours, wirelessly transmitting video images to an external data recorder.

Implantables are another area where a lot of progress is being made. For instance, a contraceptive implant that can be wirelessly controlled by women without having to make a trip to a clinic, but doctors would be able to adjust dosages remotely if the patient so requested.

Similarly a lot of research and experimentation is being conducted with neural interfaces and bionic prosthetics. They promise a new era of human medicine and enhancement that out shadow the development in the decades prior.

There is a growing population of biohackers who are obsessed with the idea of human enhancement and who are looking for new ways to put machines into their bodies. Restricting such activities will be difficult for voluntary non-commercial applications due to First Amendment protections.

5. Citations

About the privacy and security of your health records. Apple Support. (2019, February 11). https://support.apple.com/en-us/HT209519.

Apple Watch Series 6. Apple. (n.d.). https://www.apple.com/apple-watch-series-6/.

Associated Press. (2021, February 27). *Judge approves $650M Facebook privacy lawsuit settlement*. AP NEWS. https://apnews.com/article/technology-business-san-francisco-chicago-lawsuits-af6b42212e43be1b63b5c290eb5bfd85.

Canadian Maker of Smart Locks Settles FTC Allegations That it Deceived Consumers about its Security Practices. Federal Trade Commission. (2020, April 17). https://www.ftc.gov/news-events/press-releases/2020/04/canadian-maker-smart-locks-settles-ftc-allegations-it-deceived.

Clickstream data. PRIVACY IN THE WORKPLACE. (n.d.). https://cyber.harvard.edu/privacy/Module3_Intronew.html.

cnbc. (2015, January 23). *Google's Eric Schmidt: 'The Internet Will Disappear' | Tech Bet | CNBC*. YouTube. https://www.youtube.com/watch?v=Tf49T45GNd0.

Deloitte. (n.d.). *Privacy by Design Setting a new standard for privacy certification*. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF.

Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data. Federal Trade Commission. (2021, January 28). https://www.ftc.gov/news-events/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc.

Donna Marbury. (2019, May 1). *3 Reasons Why Wearables Bring New Complications for HIPAA Compliance*. Technology Solutions That Drive Healthcare. https://healthtechmagazine.net/article/2020/09/3-reasons-why-wearables-bring-new-complications-hipaa-compliance.

L. F. J. (2019, July 2). *D-Link settlement: Internet of Things depends on secure software development*. Federal Trade Commission. https://www.ftc.gov/news-events/blogs/business-blog/2019/07/d-link-settlement-internet-things-depends-secure-software.

Düking, P., Achtzehn, S., Holmberg, H.-C., & Sperlich, B. (2018, May 19). *Integrated Framework of Load Monitoring by a Combination of Smartphone Applications,*

Wearables and Point-of-Care Testing Provides Feedback that Allows Individual Responsive Adjustments to Activities of Daily Living. Sensors (Basel, Switzerland). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5981295/.

Greenberg, P. (n.d.). Security Breach Notification Laws. https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

IoT and HIPAA Compliance: Part I: Understanding HIPAA, PHI, and Medical IoT: Kajeet IoT Solutions. Kajeet, Inc. (n.d.). https://www.kajeet.net/resource/iot-and-hipaa-compliance-part-i/.

Marr, B. (2018, September 12). *19 Astonishing Quotes About The Internet Of Things Everyone Should Read*. Forbes. https://www.forbes.com/sites/bernardmarr/2018/09/12/19-astonishing-quotes-about-the-internet-of-things-everyone-should-read/?sh=8593c93e1db3.

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160118. https://doi.org/10.1098/rsta.2016.0118

New FTC Report on IoT Maintains Need for Baseline Privacy Legislation and Begins to Recognize Limitations of FIPPS in a Connected World. JD Supra. (n.d.). https://www.jdsupra.com/legalnews/new-ftc-report-on-iot-maintains-need-for-39724/.

NG, C. (2020, March 29). *5 Privacy Concerns about Wearable Technology*. Varonis. https://www.varonis.com/blog/5-privacy-concerns-about-wearable-technology/.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, *140*(4), 32–48. https://doi.org/10.1162/daed_a_00113

O'Reilly, C. A. (1996). CULTURE AS SOCIAL CONTROL: CORPORATIONS, CULTS, AND COMMITMENT. *Research in Organizational Behavior*, *8*(18), 157–200.

Privacy and Security Enforcement. Federal Trade Commission. (2019, August 23). https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

Reasonable expectation of privacy. The IT Law Wiki. (n.d.). https://itlaw.wikia.org/wiki/Reasonable_expectation_of_privacy.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477. https://doi.org/10.2307/40041279

Thierer, A. D. (2014). The Internet of Things & Wearable Technology: Addressing Privacy & Security Concerns Without Derailing Innovation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2494382

Turner, K. (2019, April 8). *Are performance-monitoring wearables an affront to workers' rights?* The Washington Post. https://www.washingtonpost.com/news/the-switch/wp/2016/08/05/are-performance-monitoring-wearables-an-affront-to-workers-rights/.