

In collaboration with
McGill University



Shaping the Future of the Internet of Bodies: New challenges of technology governance

BRIEFING PAPER
JULY 2020

Contents

3	Foreword
4	Executive summary
6	1 Part One: The internet of bodies is here
7	1.1 Range and categories of technologies
8	1.2 Data-enabled social benefits
10	1.3 Risks associated with the internet of bodies
13	2 Part Two: Governance of internet of bodies data
14	2.1 Data regulatory landscape in the US and EU
18	2.2 New governance challenges in the age of big data
21	2.3 Envisioning possibilities and options
23	Contributors
25	Endnotes

Foreword

As new technologies integrate with the human body, the opportunities – and risks – abound.



Xiao Liu
McGill University Faculty Fellow
at the World Economic Forum
Centre for the Fourth Industrial
Revolution; Wilson China Fellow



Jeff Merritt
Head of Internet of Things,
Robotics and Smart Cities,
Member of Executive
Committee, World Economic
Forum

In the wake of the COVID-19 pandemic, wearable technologies such as health and location trackers have been thrust into the public spotlight – spurring not only excitement about their potential benefits but also debate over their potential risks. Could these devices help public health authorities better predict, manage and avert future outbreaks? How might employers use data from wearable devices to safely reopen businesses? What are the implications for privacy and equity? How might this data be abused or used for other intended purposes such as public surveillance?

These questions are at the heart of new efforts by the World Economic Forum, in collaboration with public health authorities, leading technology companies and other stakeholders, to develop and pilot new approaches for the ethical treatment and sharing of health data collected by consumer wearable devices.¹

This paper aims to take these efforts one step further, looking beyond the scope of wearable

devices at the broader ecosystem of connected technologies that is coming together to create “the internet of bodies” (IoB). As with any area of emerging technology, the IoB is evolving rapidly and its future is unknown. It is for exactly this reason that careful attention and thought – not simply on the part of business but from government, civil society and the public at large – is required.

We stand at the beginning of an important public dialogue that will have major implications for public health, safety and the global economy and may also ultimately challenge how we think about our bodies and what it means to be human.

This paper does not claim to provide a comprehensive view of all of the many facets of the IoB. However, it provides a glimpse of the myriad of complex issues that can arise when the cyber and physical worlds come together. We invite you to join us in this important work to shape the development, use and impact of these technologies for the benefit of all society.

Executive summary

To realize the full potential of the internet of bodies, we need robust, up-to-date governance frameworks.



“ The internet of things (IoT) is increasingly entangling with human bodies.

The internet of things (IoT) is increasingly entangling with human bodies. This emergence and fast expansion of the “internet of bodies” (IoB)² – the network of human bodies and data through connected sensors – while offering enormous social and health benefits, also raises new challenges of technology governance.

With an unprecedented number of sensors attached to, implanted within or ingested into human bodies to monitor, analyse and even modify human bodies and behaviour, immediate actions are needed to address the ethical and legal considerations that come with the IoB. The urgency of such actions is further brought to the forefront by the global COVID-19 pandemic, with extensive IoB technologies and data being enlisted for the surveillance and tracking of coronavirus.

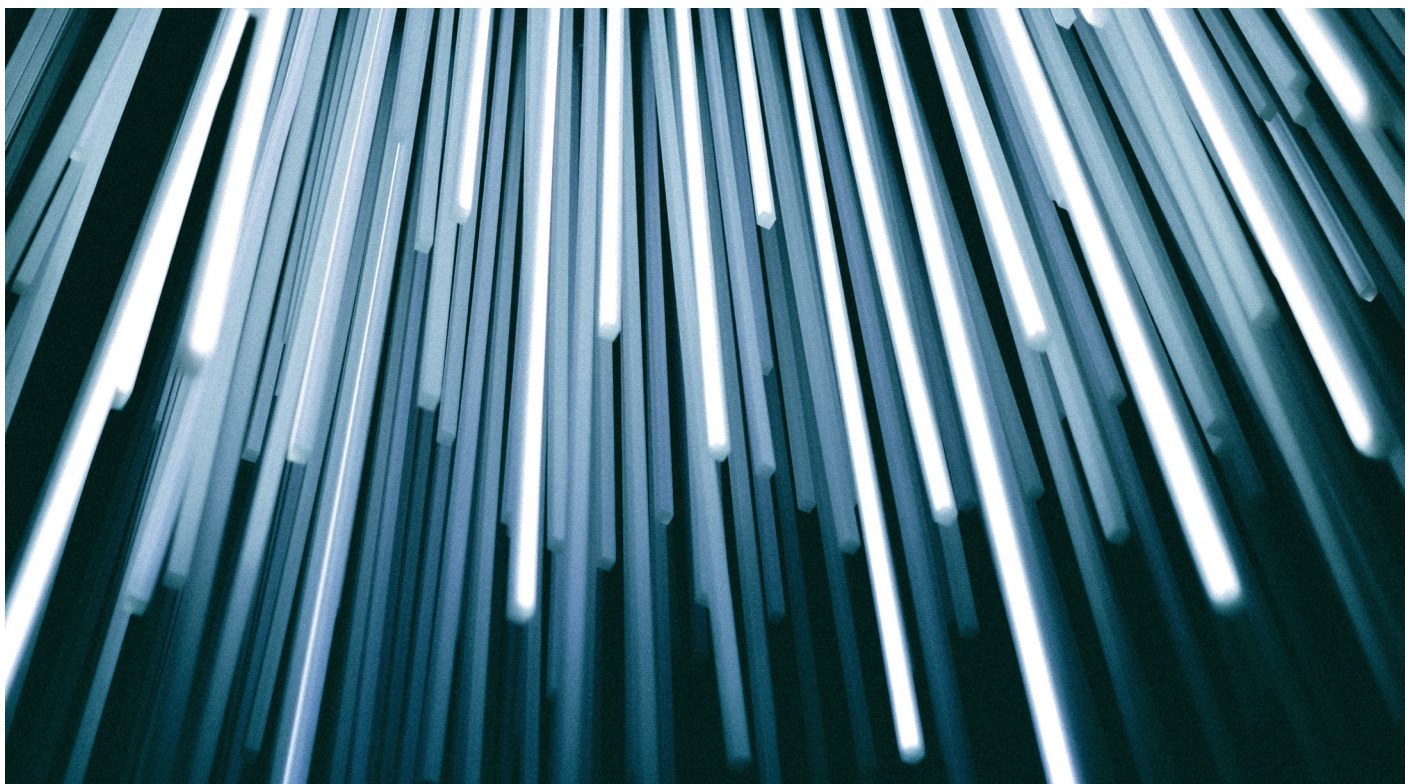
This white paper comprises two parts. Part one provides a landscape review of IoB technologies, as well as their benefits and risks. An examination of the ecosystem shows that IoB technologies are deployed not only in medical scenarios but also across different sectors, from fitness and health management to employment settings and entertainment. The accelerating convergence of consumer devices and health/medical devices also shows that the line between medical and non-medical IoB devices is blurring. This suggests that new strategies of governance are needed for IoB devices, which are traditionally subject to different regulatory agencies and rules.

It is worth noting that this white paper will not delve into gaming and virtual reality (VR) devices nor the data from them. While related, these devices raise distinct issues from the more traditional health and fitness devices.

Part two examines the governance of IoB data – focusing, in particular, on the regulatory landscape in the United States, with a comparative perspective of regulation in the European Union. This part examines current regulatory approaches to IoB data, as well as the challenges raised by the rapidly shifting ecosystem, especially the wide adoption of big data algorithms. Whereas IoB technologies also entail other issues such as the physical effects of devices on users and liability for physical harms, this paper focuses only on the governance of data generated from IoB, particularly from health and wellness IoB devices.

Two main findings for policy-makers and stakeholders are highlighted. First, broad adoption of the IoB and frequent flows of IoB data across scenarios and sectors requires robust and consistent governance frameworks in both the medical and non-medical sectors. This is particularly the case for IoB data governance as, while clinically derived data is in general strictly regulated, the regulation of consumer-generated data and other non-clinical data is often, given the sensitivity of the data, uneven in terms of coverage and strength across sectors and jurisdictions; this is the case in, for example, the United States. Second, IoB data governance approaches and data protection laws need urgent updates to address the risk of privacy, unfairness and discrimination brought about by common practices of big data analytics. This risk presented by big data analytics exists with both medical data and non-medical data, as even deidentified medical data can be reidentified or misused in a way that causes harm and discrimination to individuals and groups.

We therefore urge stakeholders from across sectors, industries and geographies to work together to mitigate the risks in order to fully unleash the potential of the IoB.



1

Part One: The internet of bodies is here

Recent advancements in the internet of things are transforming the human body into a new technology platform.



1.1 Range and categories of technologies

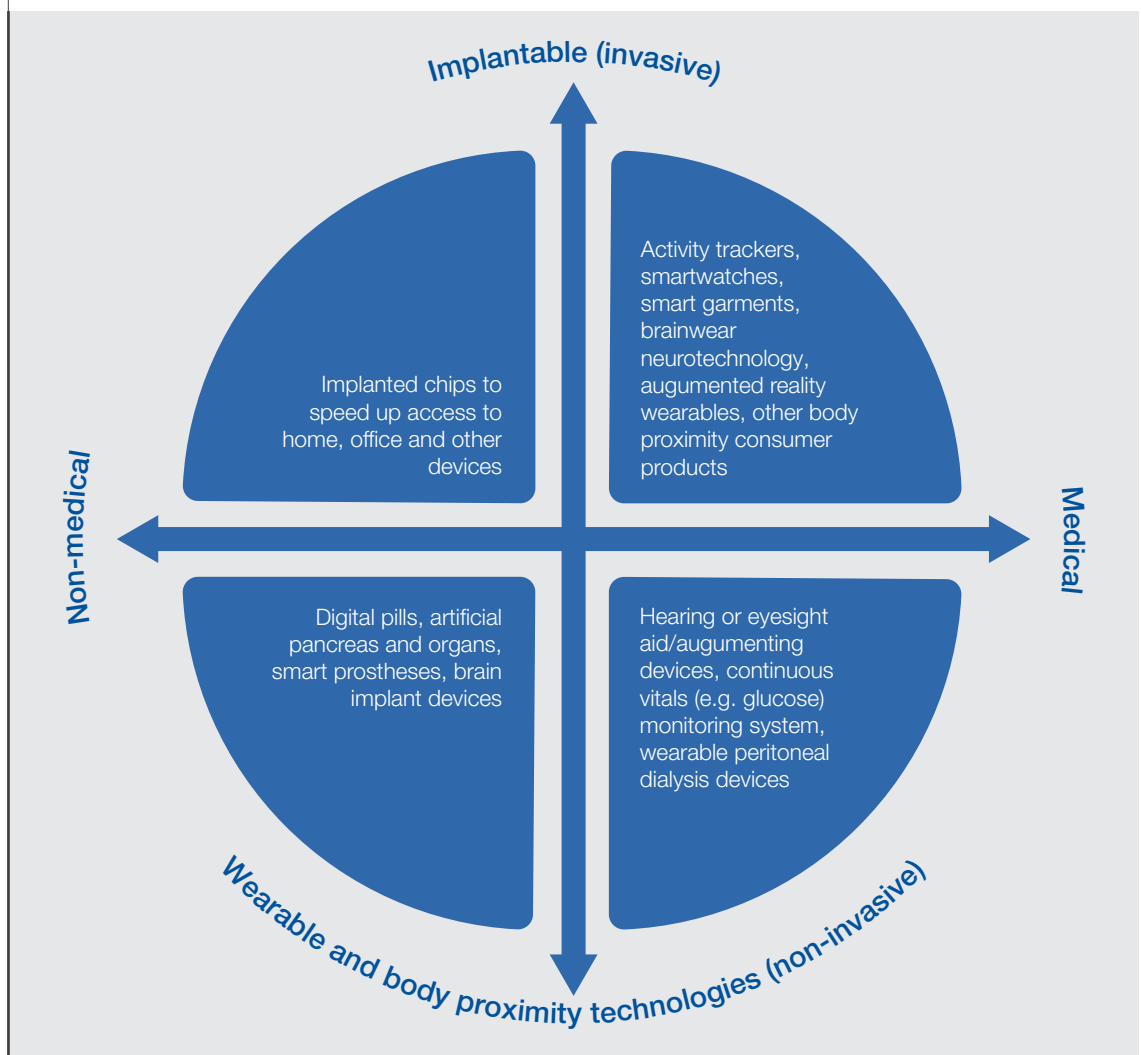
Recent technological advancements have ushered in a new era of the “internet of bodies” (IoB),³ with an unprecedented number of connected devices and sensors being affixed to or even implanted and ingested into the human body. This has turned the human body into a technology platform.⁴ The IoB generates tremendous amounts of biometric and human behavioural data. This is, in turn, fuelling the transformation of health research and industry, as well as other aspects of social life, such as the adoption of IoB in work settings, or the provision of new options for entertainment – all with remarkable data-driven innovations and social benefits. Yet the IoB also raises new challenges for data governance that concern not only individual privacy and autonomy but also new risks of discrimination and bias in employment, education, finance, access to health insurance and other important areas for the distribution of social resources.

Generally, IoB technologies include medical devices,⁵ a variety of lifestyle and fitness tracking devices,

other smart consumer devices that stay in proximity to the human body and an expanding range of body-attached or embedded devices that are deployed in enterprise, educational and recreational scenarios. It is worth noting that the IoB technologies examined here are mostly “personal devices”, in the sense that the devices always develop a relatively stable relationship with the individual body of the user over a regular, extended period of contact. This, therefore, excludes the type of biometric technologies that are installed in public and private spaces, such as facial recognition systems, fingerprint sensors and retinal scanners, which focus on collecting and processing the data of a large population or group rather than particular individuals.

As reflected in Figure 1, IoB technologies can be characterized as non-invasive or less-invasive, in the sense that they are not expected to interfere with the structure or any function of the body; or as invasive, with sensors going under the skin to be implanted into or become part of the body.

FIGURE 1 Examples of internet of bodies technologies



Invasive technologies include, for example, digital pills – a recent drug-device combination developed to deliver encapsulated medicine and monitor medication adherence – which rely on ingestible mini-sensors to be activated in the patient’s stomach, and which then transmit data to sensors, the patient’s smartphone and other data portals. Other examples of smart medical implantables include: an internet-connected artificial pancreas as an automated insulin delivery system for diabetes patients; and robotic limbs for movement rehabilitation in people with physical mobility limitations. In recent years, increasing numbers of people have chosen to implant chips under their skin, not for medical purposes but as a personal choice to speed up their daily routines and for convenience – accessing their homes, offices or other devices just by swiping their hands, for example.⁶ As part of biohacking culture, people have also sought to enhance their bodies with implanted technology, from magnets and RFID chip implants to miniature hard drives and wireless routers.⁷

Among less invasive technologies, some devices remain on the surface of the human body – these are usually called wearables. Wearable technologies are a fast expanding area, with a \$15.74 billion market in 2015, estimated to grow to \$51.60 billion by 2022.⁸ Electronic skin patches alone, which are widely adopted in medical wearables for cardiovascular monitoring, diabetes management, temperature, sweat and motion sensing and other types of biomarker monitoring, achieved more than \$7.5 billion in revenue in 2018.⁹ Non-medical wearables are a dynamic field, with products and adoptions ranging from personal fitness trackers and smartwatches to enterprise applications. These include connected glasses and helmets in employment settings for location tracking, safety monitoring and job performance improvement;

neurotechnological devices for work/learning productivity; and augmented and VR devices for entertainment and education. In addition to implantable and wearable technologies, smart sensors are increasingly appearing in ordinary consumer products such as combs, razors, toothbrushes, skin products, mattresses and others. Although they do not stay affixed to the human body at all times, these products remain in proximity to the body and collect users’ biological and behavioural data on a regular basis.

Currently, medical and non-medical IoB devices are often subject to oversight by different governance bodies and separate sets of legal regulations and rules. In the United States, for example, the pre-market approval and post-market oversight of medical devices fall under the domain of the Food and Drug Administration (FDA), while non-medical devices in the consumer domain are mainly overseen by the Federal Trade Commission. Yet, in terms of their use scenarios, the division between medical devices and non-medical consumer devices is becoming blurred. Consumer wearable manufacturers such as Apple and Fitbit look to expand their products into certified health-monitoring devices and tap into health insurers and enterprises as their customers, while traditional medical device companies are also building devices for use outside medical facilities. IoB devices are being increasingly adopted across the division of medical/non-medical categories. Smart exoskeletons, for example, are used in industrial settings to augment human performance, but also for mobility assistance, rehabilitation and other health purposes. A national survey conducted in the United States by Valencell in 2018 revealed the accelerating convergence of consumer wearables and personal health/medical devices.¹⁰ This invites a reconsideration of the line between medical and non-medical in the governance of IoB technologies.

1.2 Data-enabled social benefits

The variety and vast amount of data collected through IoB technologies is propelling transformations in health research and industry, especially with the development of the

direct-to-consumer digital health market. IoB technologies have also been adopted to enhance work safety in high-risk scenarios. Four of the more notable social benefits are detailed below.

1. Enabling remote patient tracking and reducing cross infection

The continuous monitoring of body vital signs through sensors allows healthcare providers to better track the condition of patients within and beyond medical facilities, from data regarding blood pressure, oxygen levels, glucose levels and heart rate to the person’s sleep, steps and other health-related factors. Continuous monitoring is increasingly recognized as a helpful tool to address the healthcare needs of the world’s ageing population and patients with a chronic

disease.¹¹ Recently, remote monitoring has also been used in the fight against the COVID-19 outbreak. For example, VivaLNK, a California-based connected health start-up, has designed a multipatient remote monitoring solution with Alibaba to safely monitor patient temperature, electrocardiogram (ECG), heart rate, respiratory rate and motion, and reduce the chance of cross infection for the protection of medical workers.¹²

2. Improving patient engagement and promoting a healthy lifestyle

IoB technologies facilitate the expansion of healthcare to actively engage patients beyond traditional medicine architecture. A good example is a virtual rehab programme that Kaiser Permanente started in Southern California in 2019, in which health professionals remotely monitored the exercise and medication-taking habits of enrolled patients recovering from cardiac events. Wearing smartwatches enables

patients to share their vital and activities data with their care providers, who interact with them regularly. The enhanced relationship between patients and care providers and the flexibility of the remote programme beyond traditional clinic settings improved the completion rate of the rehab programme from less than 50% to 87%, effectively lowering readmission rates, and also reducing medical costs.¹³

3. Advancing preventive care and precision medicine

The data provided by IoB technology enables physicians to spot diseases early and offer preventive measures. Also, the volume and variety of data may help advance precision medicine research by linking individual lifestyle and environmental data with genetic and biologic data, providing deeper insights into the drivers and treatments of disease. Consumer wearables provide new types of data and possibilities in scientific research and clinical trials. From 2012 to 2017, more than 500 published studies explored the use of Fitbit devices, with

research conducted across a variety of different study populations and environments.¹⁴ New and complex data sources beyond traditional clinic settings can also extend research from individual health to population health to understanding how human behaviour, characteristics of communities, living and environmental conditions, as well as institutions and policies, all contribute to the general health of a social group. This can potentially help alleviate existing and potential equity issues in marginalized groups' access to health resources.

4. Enhancing workplace safety

Beyond health applications, IoB technologies are also being adopted in hazardous workplaces such as construction sites, mines and factories to track worker location, oversee environmental risks, reduce exposure to musculoskeletal injuries or other harms, and mitigate risks by issuing information remotely.¹⁵ High-quality real-time sensor data provides guidance to workers under complicated

and fast-shifting conditions, and improves safety monitoring. Advancements in neurotechnology have also delivered brainwear devices that can measure airline pilots' and drivers' alertness to improve travel safety. Biometric sensors, from caps and vests to wristbands and eyewear, are becoming lighter and cheaper, and can measure drivers' fatigue levels and alert them to pull off the road when drowsy.¹⁶



1.3 Risks associated with the internet of bodies

Along with the social benefits and innovations enabled by data from the IoB come new risks associated with the misuse of data that contains intimate details of personal health and behaviours.

Admittedly, IoB technologies share many concerns with the internet of things, such as consumer trust, safety, security and interoperability. Several aspects of particular concern are detailed below.

1. Interoperability and data accuracy

Issues of standardization of data and interoperability of technologies present important obstacles in combining and benefitting from different types of data from varied sources to improve medical care and advance research. With millions of devices in the health ecosystem deployed to monitor the human body, from the hospital bed to anywhere the IoB devices go with the body to which they are attached, the dominance of proprietary and closed communication methods results in vendor lock-in and a lack of interoperability between these devices at the platform and technical level. The lack of a standardized platform to pull continuous streams of data from different devices constrains the use of that data to deliver valuable insights unless all data sources are inherently from interoperable devices. Increasingly, we are seeing interoperability between wearables and consumer platforms, but this is more difficult to ensure when it comes to combining that data with data from medical records, for example. The Health Insurance Portability and Accountability Act (HIPAA) in the US supports portability of health information such as

medical records, but because wearables collect data that is not under the remit of HIPAA, there is no onus on the manufacturers of wearables to ensure that level of interoperability of system or portability of data.

Besides interoperability, data accuracy is a concern, especially with consumer fitness devices. Currently, medical devices and non-medical devices are subject to different regulatory and pre-market approval standards. However, as consumer tracking devices are becoming integrated in healthcare – for example, to monitor heart rate and energy expenditure in patients with cardiovascular disease – the issue of whether their measurements reach a level of clinically acceptable accuracy needs assessment and discretion.¹⁷ The replacement of medical-grade devices with consumer devices may run the risk of misdiagnosis such as false alarms and overtreatment.¹⁸ We see consumers increasingly relying on wearables to self-assess their own health based on data from wearables, without FDA or medical oversight, and as such without guidance.

2. Cybersecurity and privacy

There is increasing awareness of the vulnerability of wearables and medical IoT devices to hacking and cyberattacks, which expose human lives to potential physical harm and privacy risks. Globally, healthcare cybersecurity breaches in 2018 accounted for 25% of 750 reported incidents, more than any other industry.¹⁹ The issue is no less grave for consumer devices. Researchers have found serious security flaws with children's smartwatches, which hackers can use to track children, gain access to audio, and make phone calls to them.²⁰

Privacy is one major factor affecting consumers' trust and adoption of IoB devices. Increasing adoption of IoB devices beyond traditional medical facilities also raises new concerns about security and privacy, while technical standards and policies are yet to reflect these new challenges. For example, an interactive map showing the whereabouts of people who use wearable fitness devices revealed information about the locations and activities of soldiers at US military bases. Taken as an aggregate, this is highly sensitive information because it describes military movements even though personal identifier information is removed from the published data.²¹ At a consumer level, geolocation data derived

from a wearable can point to commuting patterns or other information that could be misused in the wrong hands. Amid the global outbreak of COVID-19, with the enlisting of data for coronavirus tracking and the relaxation of enforcement regarding health data in the US and other countries, the privacy of health data has generated serious concerns. The (im)balance between data privacy and the transparency required to tackle a public health emergency continues to be a contentious topic. For example, the use of smart thermometer data for health surveillance and to create a "US health weather map" has raised alarming privacy concerns. Some thermometer companies are using this personal information to market and sell the data to third-party companies.²²

To address these issues regarding wearables in order to standardize the approach taken by manufacturers globally, the Institute of Electrical and Electronics Engineers (IEEE) and its Standards Association have been working with the FDA, National Institutes of Health, and universities and industry since 2016. Through the initiatives, the IEEE and its community has established TIPPSS (trust, identity, privacy, protection, safety and security) as the principles to ensure patient safety.²³

3. Risks of discrimination and fairness in data analytics

Emergent practices in relation to the handling of data derived from IoB devices signal potential alarming discriminations and bias against individuals. When this user-generated, biologically derived data is combined with data from myriad other sources, such as retail stores, consumer product and service companies, finance services and government institutions for data analytics, abuse can occur. Algorithmic analytics can be used to make important decisions in areas such as insurance, employment, finance, education, criminal justice, social services and the allocation of other types of social resources, all based on data derived from IoB devices. Profiling and grouping based on inaccurate or incomplete data, proxy data and the generation of sensitive data from inferences can result in biased policies and decision-making that affect not only individuals but also groups and vulnerable populations, even though data processors and decision-makers sometimes may not realize the implicit bias or potential harm. Several examples of areas in which this discrimination and bias may be seen are noted below.

- **Discriminatory insurance policies:** The use of IoB data with minute details of individual health conditions and life habits in insurance could fragment the solidarity foundation of insurance and shake its socioeconomic and ethical basics. Some insurers have already dug into vast amounts of personal data, ranging from home addresses and ownership, and education levels, to lifestyle data such as dietary habits, daily activities and exercises. The information is fed into computer algorithms to assign each individual a risk score for decisions regarding healthcare insurance, but also in other types of insurance, such as life insurance, disability insurance and even in areas not directly related to health, such as financial loans.²⁴ The data from IoB technologies often includes fine-grained details of personal life as well as physical and mental health. The misuse of this data could lead to discriminative insurance policies and prices, making it harder for marginalized populations to access basic healthcare, and other types of insurance.
- **Discrimination and bias in employment:** The adoption of wearables and IoB devices in employee wellness programmes and in employment scenarios creates new concerns about employee privacy and workplace surveillance. With employers using devices and algorithms to monitor and direct employees' movements, communication and behaviour patterns, relatively weak regulations in this area offer limited legal protection. This can expose workers to higher risks of misuse of data and black-box algorithms that may lead to biased decisions regarding hiring, promotion and retention.²⁵ For example, hiring algorithms

and predictive technologies are found to replicate institutional and historical biases, but such biases are less easy to detect due to the lack of transparency of the algorithms and the sources and quality of data used for such algorithm training.²⁶ The increased risks of privacy intrusion and unfairness have already generated opposition from employees, unions and activists.²⁷ In 2018, West Virginia teachers went on strike to demand the removal of a workplace wellness programme that was criticized for penalizing members for not scoring "acceptable" levels on biometric measures.²⁸ Workers at UPS, McDonald's and Amazon warehouses have also protested against the exacerbated work stress and precarity imposed by management through intensive data-collecting trackers, and requested new rules regarding employers who use tracking data to discipline employees.²⁹

- **Public policy that creates and/or reinforces social inequality:** Policy-makers are increasingly using new data sources and data analytics for decision-making in public policy such as health, disaster response, urban design, national security, economic development and other areas. Potential bias in the types and quality of data and algorithms may intentionally or unintentionally create and reinforce social inequality, limiting access for certain social groups to health and other public resources. New sources of data from mobile phones and IoB devices, for example, have been adopted to track and predict the outbreak and transmission of diseases. Yet, when deployed without attention to the potential biases of data and algorithms, there is a risk that data may remove an epidemic from its political and societal context, and, in particular, affect the lives of vulnerable populations. In the case of the 2014 Ebola outbreak, for example, many humanitarian organizations active in Africa encouraged governments, charitable foundations, technology companies and mobile networks to share data. But studies show that they lacked the data-modelling capabilities, professional technology implementation standards and enforcement capacity to define or protect the public interest, which resulted in the violation of basic human rights and aggravated the inequality gap in terms of accessing disaster assistance resources.³⁰

The adoption of data analytics in decision-making involves unprecedented volume, velocity and variety of data, among which the data from IoB technologies is combined with those from other sources for cross-reference purposes. This suggests that the collection and use of IoB data often goes beyond the health sector; and on the other hand, data that is not directly health-related,

such as social media data, can also be used to generate analytics relating to individual and group health. These emergent practices and potential risks raise new challenges in governing the data generated by the expanding range of IoB networks. It is already difficult to guard data rights and ensure transparency and fairness in the age of big data, and the specific challenges that IoB technologies create in this space mean that they need to be considered as part of that debate.

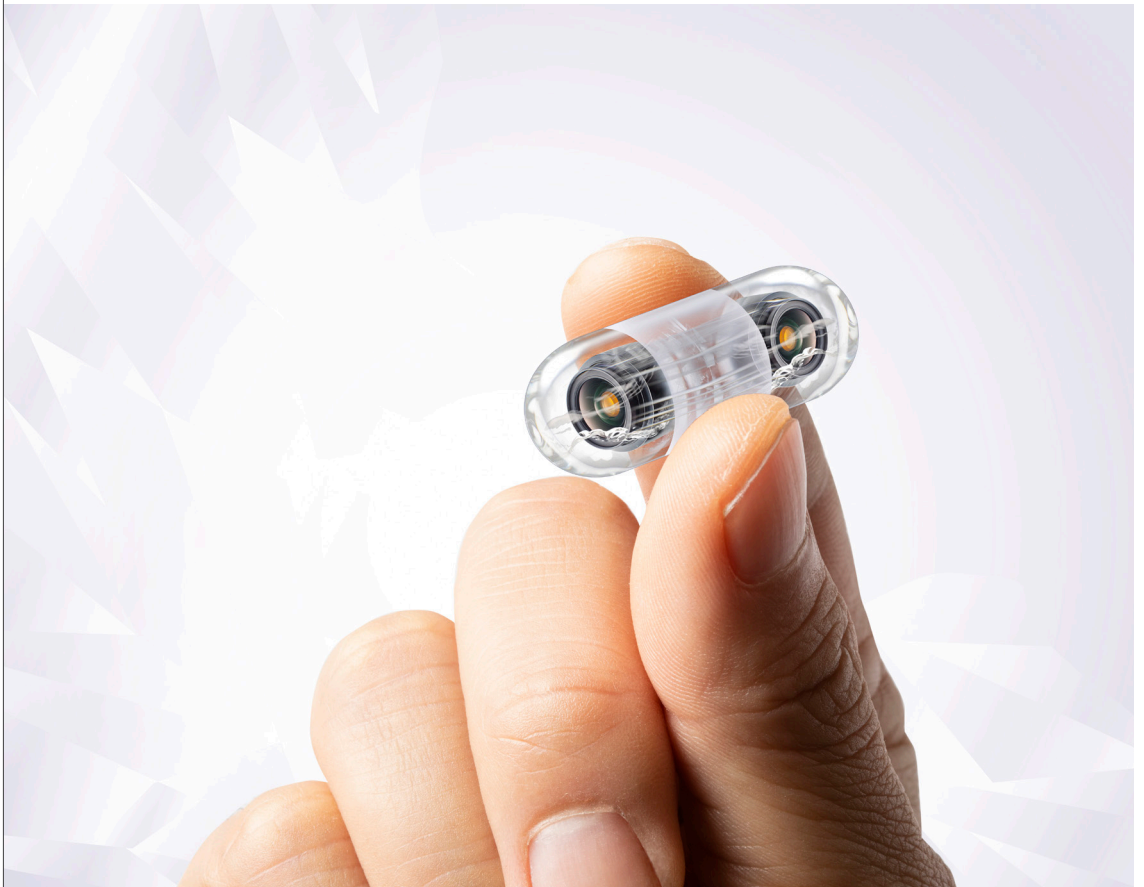
As will be discussed in the following section, while clinically based data is, in general, subject to strict regulation, the governance of data from health-based lifestyle and other non-medical devices is more uneven due to the divergence in data regulations across sectors and under different jurisdictions. It is suggested that laws governing the collection of medical data are largely insufficient to address the security, privacy and discrimination risks arising from the processing of IoB data.



2

Part Two: Governance of internet of bodies data

Current regulations address some but not all of the many risks introduced by IoB data.



While the manufacturing and security of loB devices may be subject to different government agencies and related rules (such as Federal Communication Commission [FCC] regulations and guidelines for manufacturing IoT devices in the United States), the focus here is on the collection, transfer and use of loB data, particularly the risks of discrimination

that come along with data analytics. As discussed, the adoption of loB technologies is not limited to the medical applications space but spans different sectors. This is further complicated by the practice of data analytics, which constantly generates new data by combining and analysing different sources of data, regardless of its origin.

2.1 Data regulatory landscape in the US and EU

“ In both the US and the EU, there remains a gap between anti-discrimination laws and the new risk of discrimination arising from data-driven inferences, profiling and grouping.

This section examines the regulatory landscape regarding loB data in the United States, with a comparison to the Europe Union. Relevant loB data regulations in the US are sectoral, with separate laws for different types of information, users and situations. This is complicated for data controllers and users to navigate, and the coverage and strength of data protection may diverge significantly across sectors and by state and local regulations. While medical data is often considered sensitive and thus strictly regulated, non-medical data from consumer devices is

not always subject to the equivalent strength of protection, even where physiological data, such as from fitness devices, is concerned. In Europe by comparison, the General Data Protection Regulation (GDPR) is a non-sectoral and technology-neutral data regulation that provides guidelines for the procedures for collecting and processing personal data. In both the US and the EU, there remains a gap between anti-discrimination laws and the new risk of discrimination arising from data-driven inferences, profiling and grouping.

Extant regulations in the United States

The US does not have a comprehensive data protection law regulating all aspects of information privacy or security. Data generated from loB technology could be subject to three separate

bodies of law and regulation: sector-specific federal laws and regulations; federal-level anti-discrimination laws; and state-level, county-level and local laws and regulations.

1. Relevant federal laws and standards in the US

- **Health Insurance Portability and Accountability Act (HIPAA):** The HIPAA, supplemented by the Health Information Technology for Economic and Clinical Health Act (HITECH Act) in 2009, regulates the use and disclosure of “protected health information” (PHI) by covered entities. Covered entities include health plans, healthcare providers, healthcare clearing houses and their business associates. The HIPAA also provides guidance regarding two methods that can be used to satisfy the privacy rule’s deidentification standard: Expert Determination and Safe Harbor.³¹ HIPAA’s privacy rule does not apply to deidentified data, nor any data beyond PHI handled by covered entities.
- **Federal Trade Commission (FTC) Act:** The FTC Act, enforced by the Federal Trade Commission, prohibits companies from engaging in deceptive or unfair acts or practices, including failing to comply with an entity’s own privacy policy among others.³² This makes the FTC Act the primary federal statute applicable to the privacy and security practices surrounding consumer loB devices.
- **The Fair Information Practices Principles (FIPPs):** Administered by the FTC, FIPPs guide the interpretation of data protection that characterizes the sectoral approach to US privacy law. What were originally broad consensus principles as standards have evolved into a more prescribed set of rules applied in different privacy contexts. They are the foundation of the social group and context approach, ranging from medical data (HIPAA) and financial data (Gramm-Leach-Bliley Act [GLBA]) to children’s rights (Children’s Online Privacy Protection Act [COPPA]), students (Family Educational Rights and Privacy Act [FERPA]), consumers (e.g. Telephone Consumers Act [TCPA]), and driver’s privacy (Driver’s Privacy Protection Act [DPPA]).
- **Gramm-Leach-Bliley Act (GLBA):** The GLBA regulates personally identifiable financial information that is provided by, results from or is otherwise obtained in connection with consumers and customers who obtain financial services, including insurance providers. It limits the disclosure of non-public personal information collected by a financial institution. It does not restrict the use of personal information or big data analytics for personalizing insurance contracts.³³

“ In the US, the Civil Rights Act of 1964 prohibits discrimination based on individual characteristics such as race, religion or sex.

- **The Fair Credit Reporting Act (FCRA):** The FCRA regulates any “consumer reporting agency” (CRA) that furnishes a “consumer report” to be used primarily for assisting in establishing a consumer’s eligibility for credit, where the report pertains to the person’s creditworthiness, credit standing, character, general reputation, personal characteristics, model of living etc.
- **The Federal Policy for the Protection of Research Subjects (Common Rule):** Common

Rule applies to research involving the collection or study of existing data, documents, records, pathological specimens or diagnostic specimens, but anonymous or deidentified information is expressly exempt from regulation.

- Besides these, other specific regulations, such as the Family Educational Rights and Privacy Act (FERPA), COPPA and the FCC Broadband Consumer Privacy Rules, may be relevant to the sharing and use of IoB-related data in varied specific contexts.

2. Federal-level anti-discrimination laws in the US

Under the US Constitution, a common characteristic of a group, such as skin colour, gender or sexual orientation, ought not to form the basis for unequal treatment. The Civil Rights Act of 1964 prohibits discrimination based on individual characteristics such as race, religion or sex. Relevant laws concerning discrimination against people with certain characteristics include the following:

- **Americans with Disabilities Act (ADA):** The Americans with Disabilities Act of 1990 was enacted to eliminate discriminatory barriers against qualified individuals with disabilities, individuals with a record of a disability and individuals who are perceived as having a disability. Yet it does not reach people who are currently healthy but are perceived as being at high risk of becoming sick in the future, and hence it does not regulate a number of parties, such as employers, financial institutions, marketers and educational institutions, that are likely to have an interest in individuals’ predictive health data.³⁴

- **Patient Protection and Affordable Care Act (ACA):** The ACA aims to guarantee non-discrimination in connection with programmes funded under the ACA. It prohibits discrimination on the basis of race, colour, national origin, sex, age or disability in certain health programmes and activities. When interpreting the ACA’s underlying race and sex statutes, courts have held that they bar only direct but not indirect discrimination.

- **Genetic Information Nondiscrimination Act (GINA):** The GINA protects US residents from genetic discrimination in healthcare insurance coverage and employment contexts. However, it excludes other forms of insurance such as life insurance, long-term care and disability insurance. It does not address discrimination risks in education, finance (such as mortgage lending) or housing.

Other anti-discrimination laws and regulations, such as the Age Discrimination in Employment Act and the Pregnancy Discrimination Act, may be relevant in specific contexts.

3. State-level and other local laws and regulations in the US

State-level, county-level and municipal laws and regulations, and other sector-specific regulations, are applicable in respective jurisdictions. Relevant examples include the California Consumer Privacy Act (CCPA), the Illinois Biometric Privacy Act (BIPA) and the New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), among others.³⁵ The CCPA is the first law in the US to set up a comprehensive set of rules regarding consumer data, and applies to any company that operates in California and meets one of the defined thresholds. The SHIELD Act requires any person or business owning or licensing computerized data that includes the private information of a resident of New York (“covered business”) to implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information. The BIPA is among the most comprehensive state biometric privacy laws, and

allows individuals to file suit for the violation of their privacy even if the individuals do not suffer any actual harm. But there are also failed state privacy laws. For example, early in 2020, for the second year in a row, data privacy legislation failed in Washington State. There are also other county and city regulations related to biometric data. For example, although facial recognition systems installed in public spaces are excluded from the scope of IoB technologies examined in this white paper, San Francisco and Boston’s facial recognition bans demonstrate local approaches to regulating biometric data. In general, state and local-level governance of IoB and biometric data is dynamic and constantly evolving.

In addition to government regulations, trade groups and industry-supported non-profits, such as the Consumer Technology Association and

the Future of Privacy Forum, have developed a number of guidelines, codes of conduct, principles and methodologies for privacy and data regulation

of consumer wellness and wearable products.³⁶ These programmes offer a patchwork of industry self-regulations.

TABLE 1 Risks and gaps in relevant examples of policies in the US

Issues and risks	Examples of relevant policies to IoB data	Major gaps	Examples of relevant local regulations
Limited scope of “health information”	HIPAA	No coverage on data from direct-to-consumer medical devices and consumer devices that are not handled by covered identities; no coverage on inferences on health information	California Medical Information Privacy Act (CMIA) expands health information protection duties to providers of software, hardware and online services
Risks of discrimination in finance and insurance	FCRA; GLBA; GINA (health insurance)	Uneven in addressing the use of health and health-related information in life insurance, long-term care insurance and other types of insurance; few measures to address the risks of big data analytics	CCPA (does not impose legal obligations on government agencies, but may be relevant when involving disclosure about third parties) BIPA (regulates how private entities collect, use and share biometric information) SHIELD Act etc.
Risks of discrimination in employment	Constitutional rights (apply to federal and state governments); GINA; ADA; the Pregnancy Discrimination Act	Few measures to address predictive health data; varies between public and private sectors; exemption made to employer-offered wellness programme in which an employee voluntarily participates	California Medical Information Privacy Act (CMIA) expands health information protection duties to providers of software, hardware and online services
Risks of discrimination in public policy	Fourth Amendment to the US Constitution (prohibits government from unreasonable searches and seizures, including both physical searches and searches for personal information through wiretaps and access to company records)	Complicated landscape in accessing personal information for law enforcement and national security	

4. European Union perspective and GDPR

The fundamental rights of protection of personal data and the right to private and family life, home and communications are enshrined in the EU Charter of Fundamental Rights.³⁷ EU data protection and privacy laws are built upon the distinction between personal data and non-personal data, with higher-level protection for special categories of personal data, such as health data.

The EU GDPR, effective since 2018, applies to the collection, transfer and processing of personal data. It is complemented by a separate ePrivacy directive³⁸ that ensures the privacy of data in transmission, e.g. on network infrastructure between two parties, and can include ensuring the privacy of metadata as well as personal data.

Vital provisions that are of relevance to IoB data include the following:

- **Data protection principles:** The GDPR presents a set of principles to follow when collecting, processing and storing personal data, including: purpose limitation, data minimization, storage limitation, accuracy, integrity and confidentiality (security), accountability and lawfulness, fairness and transparency. However, the vague definition of “fairness” compromises an effective protection against the risk of discrimination resulting from data analytics. Furthermore, the legal basis for the collection of personal data from a person needs to be determined by the data processor. Sometimes, this relies on consent and sometimes it relies on a legitimate interest or the performance of a contract, to name just three possibilities under Article 6.
- **“Data concerning health” as a special category of data:** “Data concerning health” is defined in the GDPR as “personal data related to the physical or mental health of an individual, including the provision of healthcare services, which reveal information about his or her health status”.³⁹ Distinct from HIPAA’s definition of personal health information, lifestyle and well-being data from consumer devices should be considered health data,

especially when it is processed with the aim of monitoring the health or well-being of an individual. In addition to the legitimate grounds for the processing of personal data listed in Article 6, Article 9 lists the conditions for processing special category data, which include: explicit consent of the data subject for the assessment of the working capacity of the employee; reasons of substantial public interest; public health; research etc.

- **Right to contest automated individual decision-making:** Article 22 articulates the right of the data subject “not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her”,⁴⁰ and exceptions to such rules. In addition, automated decisions must not be based on special categories of data.

Beyond the GDPR, EU non-discrimination law, both primary law (the EU Charter of Fundamental Rights) and secondary law, may be relevant when it comes to the use of data for discriminatory decisions in areas such as employment, the welfare system and access to goods and services. Some examples of secondary non-discrimination law include the Racial Equality Directive (2000/43/EC), the Gender Equality Directive (recast) (2006/54/EC)⁹⁴ and the Gender Access to Goods and Services Directive (2004/113/EC)⁹⁵, but there is sectoral divergence.⁴¹ While the European Union Charter of Fundamental Rights and other laws target the implementation of the principles of equal treatment, exceptions have been created, where, for example, in financial services, client segmentation based on actuarial factors was exempted from the scope of existing discrimination law. Furthermore, while the use of identity for customer segmentation has been declared unlawful in the European Court of Justice, the use of lifestyle data for generating inferences and risk scores raises new challenges to transparency and fairness. In a report published in 2019, Finance Watch identifies data from connected health devices as a high-risk area for discriminatory insurance policies and social exclusion.⁴²



2.2 New governance challenges in the age of big data

The issues raised by expanding IoB technologies, and the gaps in the regulatory landscape, represent much broader concerns about the risks of data privacy and

rights as well as new challenges to data protection in the age of big data analytics. Six of these pressing governance challenges are outlined below.

1. Defining “health data”

IoB technologies have generated high volumes of physiological and biometric data that far exceed traditional definitions of health information, which mainly refers to patients’ medical records and biospecimens obtained in clinical settings. Consumer wearables and body-proximity technologies have proved valuable for capturing health and wellness data beyond medical facilities. There are also other types of data, such as retail records and social media data, that could be used to deduce details about individuals’ physical and

mental health.⁴³ In a widely reported incident, the retail chain Target figured out that a teenage girl was pregnant before her parents knew through analysis of her shopping records.⁴⁴ While health data regulations such as the HIPAA traditionally focus on patient information within traditional health architecture, the blurred boundaries of health data renders inadequate the custodian-specific (where and how data is created) approach of data regulation to address frequent flows of data across sectors and contexts.

2. Balancing data utility and extant data protection principles

The proliferation of IoB technologies, and the volume, velocity and variety of data involved in analytics and predictive modelling, is the most prominent and powerful aspect of big data. Basic principles of data protection such as “data minimization” and “purpose limitation” may run counter to big data practices that require massive quantities of data for algorithm training, and often involve repurposing and combinatorial use of data.

In practice it is also difficult to foresee the purposes of the processing and secondary use of data. These principles, which have been guiding privacy and data-protection policies in both Europe and the US, are largely derived from the Fair Information Practice Principles (FIPPs) developed in the 1970s. These principles need to be reassessed and updated to adapt to the new practices of big data analytics.

3. Governing personally identifiable information (PII) and personal data

As data protection rules historically focus on personally identifiable information (PII) and personal data, the threshold of identifiability and the possibility of reidentification become crucial to defining privacy risks. Existing requirements of deidentification, such as the HIPAA Safe Harbor Provision that requires the removal of 18 types of identifiers, have been criticized for hampering research activities without offering effective privacy protection.⁴⁵ Effective use of data for health research may require linking the multisourced data so that data describing an individual located in one source is linked to those in other sources. On the one hand, the “one-size-fits-all” approach to deidentification may affect data integrity and utility in research, and on the other hand it has been

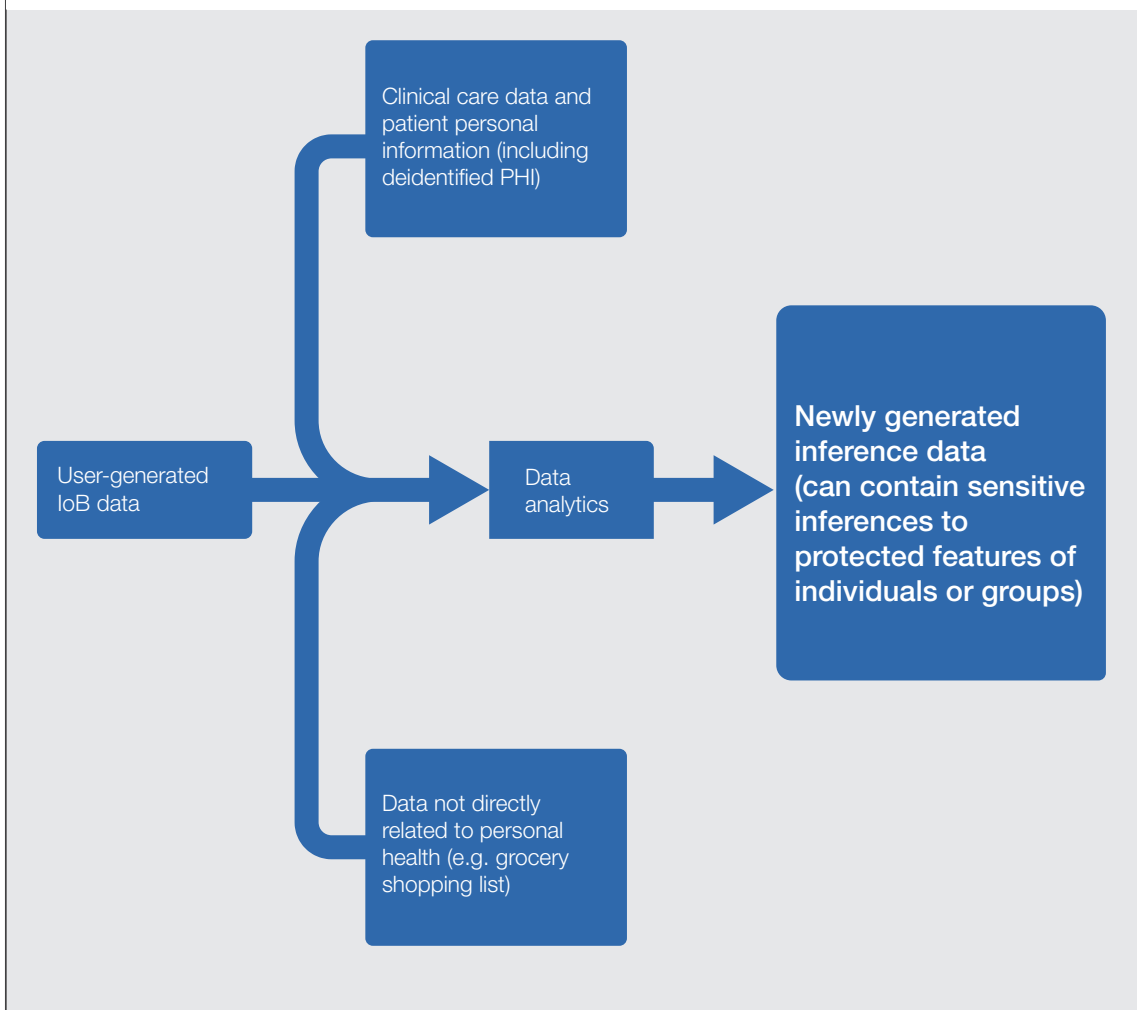
proved insufficient in protecting privacy, not only because deidentification doesn’t work for genomic data but also because deidentified data could potentially be reidentified by cross-correlating data elements with external datasets, such as voter registration records, commercially available databases and other sources.⁴⁶ It is estimated that between 63% and 87% of the population of the United States could be uniquely identified using only their gender, zip code and date of birth.⁴⁷ Yet the classification of data that meets the deidentification standard as non-personal data will place it beyond HIPAA data privacy rules, even though, in reality, the boundaries of personal identifiable information are becoming fluid in the big data environment.

4. Categorization of “sensitive data”

Some data is more sensitive than other data, and even non-personal metadata can be sensitive in nature. With big data analytics, inferences about someone’s health conditions can be drawn from indirectly related health data; health and behavioural data from loB technologies can also be used to make inferences for predictions and decision-making in areas such as insurance, employment and finance. Public and private agents may draw “high-risk inferences”, meaning inferences drawn from big data analytics that are privacy-invasive or have low verifiability, for claims and decisions that can harm the interests of individuals and groups.⁴⁸ Profiling and inferential analytics can generate sensitive information such as racial or ethnic origin from data classified as non-sensitive information by existing regulations, such as by zip code. For example, affinity profiling – the grouping of people according to their inferred or correlated characteristics rather than known personal traits – raises the risk of what the Oxford Internet Institute data protection expert Sandra

Wachter calls “discrimination by association”, a situation in which a person is treated significantly worse than others based on the person’s assumed relationship or association with a protected group. Such affinity profiling therefore generates sensitive inferences regarding the person’s ethnicity, sexual orientation and other personal traits, even though such profiling is not obtained through the processing of protected sensitive data (e.g. special categories of data in GDPR).⁴⁹ Furthermore, the degree of sensitivity also depends on the purpose and context of data use. For example, information about a person’s age may not be deemed sensitive but could be used against them in important decisions on insurance and hiring. This is not to deny that medical data and other loB data directly linked to protected features are sensitive, but to raise attention: Big data inferential analytics renders inadequate the regulatory measures that solely rely on limited and static categories of sensitive/non-sensitive data at the time of their collection and before they are processed.

FIGURE 2: Risks of sensitive inferences



5. “Privacy self-management” and consent

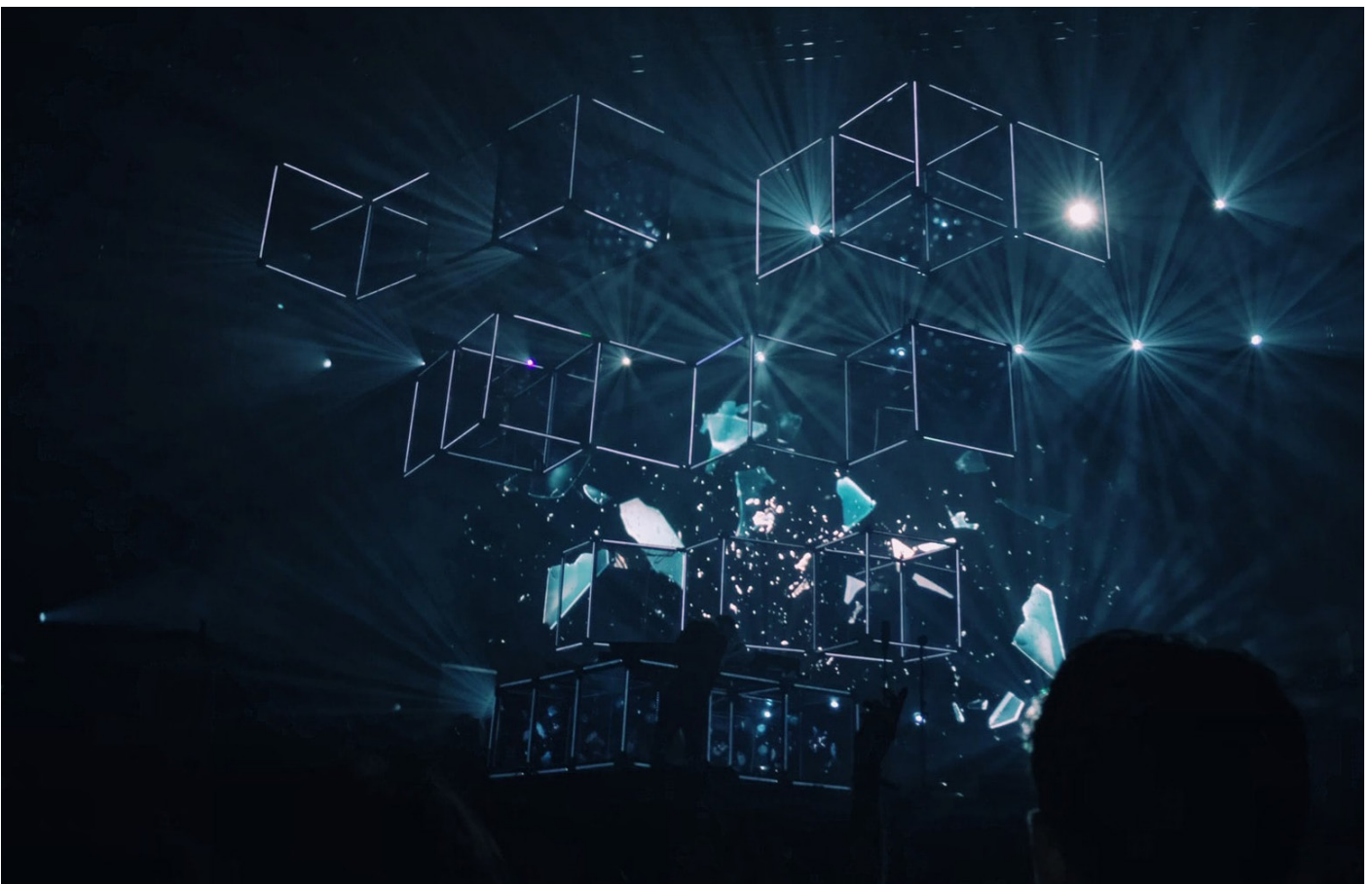
It has become increasingly challenging for data subjects to trace what data is being collected and how their data is used due to processed data's mutable character and the opacity of algorithmic codes. The mechanism of “notice-and-consent” addresses neither the opacity of algorithms and predictive modelling,⁵⁰ nor the knowledge and power asymmetries between data subjects and data controllers. Therefore, the notice-and-consent model, emphasizing the “privacy self-management” of individuals, often falls into legal formality

because of the purposefully arcane language and the impossibility of tracing and handling frequent data flows and the unpredictability of processing outcomes. Furthermore, interconnected big data environments may exhibit “privacy interdependence”, situations in which one's privacy is affected by the decision of others.⁵¹ A good example of this is genetic data, which is partially shared with family members, and the revelation that one person's genetic data can affect other people's rights of choice and privacy.

6. Algorithm grouping to individual-based data protection

Algorithmic classification systems raise a challenge to existing theories and policies of privacy, as current policies mainly focus on individual-level and personal identifiable information, which means individuals' claims to manage data about themselves often end once identifiers are removed from the data. Yet grouping occurs more through algorithmic forms of impersonal categorizations of behaviour and prediction. The identity tokens created through grouping are often not reducible to, or owned by, individuals of the group. Decisions and policies based on algorithmic grouping will nonetheless affect the interests of individuals in the group even though such grouping does not specifically target identifiable individuals. Consumer group profiling, scoring solutions and predictive

policing applications are several examples.⁵² This may lead to price discrimination depending on the assignment of consumers to a specific cluster, or geographical discrimination that affects people of certain neighbourhoods particularly in cases of, for example, the adoption of predictive policing solutions that come with unchecked algorithm biases.⁵³ The combination of different types and sources of data for analytics puts individuals into groups that were previously non-apparent or non-existent.⁵⁴ It may create groups that do not necessarily resemble historically protected groups, in which case existing non-discrimination laws may fall short. Potential victims may never be aware of the grouping and thus be unable to raise a claim under non-discrimination law.



2.3 Envisioning possibilities and options

To tackle these new challenges of technology governance related to the IoB, multistakeholder action is urgently needed. The following section

outlines a menu of possible approaches, from regulatory to technological, to help mitigate these risks in order to fully unleash the potential of the IoB.

1. Building a robust and consistent system of governance around the internet of bodies

As the internet of things is increasingly evolving to be connected with human bodies, a robust and consistent system of governance is needed to address the risks of the expanding IoB. This means that, for example, in the US context, a new governance strategy should be formed across the conventional division of medical and non-medical fields to address the broad dynamics of IoB technologies and data. Some experts suggest combining the powers of the FDA and FTC, along with the Consumer Product Safety Commission and the Consumer Financial Protection Bureau.⁵⁵ Senators Amy Klobuchar (D-MN) and

Lisa Murkowski (R-AK) introduced the Protecting Personal Health Data Act in 2019, and proposed the establishment of a national task force entrusted with protecting health data.⁵⁶

The governance of the IoB, as in the case of the IoT, relies on not only policy-makers and regulators but also trade groups, industrial associations, patient groups, users and citizens, civil society and other forms of multistakeholder cooperation, as IoB technologies are germane to the protection of fundamental human rights in a connected world.

2. Addressing the outcomes of data inferences and analytics in data protection

As discussed above, current data protection regulations mostly focus on ensuring that data is lawfully obtained, and that its processing meets the requirements of lawful grounds. But in general, extant regulations fail to address the risks of the outcomes of algorithmic deployment in all cases. To put it in a simple way, they concern mainly the input data, rather than the new data generated from the algorithm. AI and data regulation should address risks of privacy and discrimination in data inferences and algorithm analytics. Data protection experts have demonstrated that advances in big data analytics demand new protections for group privacy, addressing privacy interests of ad hoc groups formed by algorithmic classification.⁵⁷ Different from the conventional concept of a group, algorithmically generated groups are characterized by a highly dynamic instead of a stable membership, and individuals clustered in a group may not even be aware of their membership.

It therefore remains an urgent task to address the collective data rights of algorithm-generated groups, which are not equivalent to, or encompassed by, individual privacy.⁵⁸

Sandra Wachter and Brent Mittelstadt advocate “a right to reasonable inferences” to address the accountability gap posed by “high-risk inferences” and the risk of “discrimination by association”.⁵⁹ Wachter points out that to effectively address the risks of inferences, a robust data protection law should be supplemented with agile sectorial laws, especially in high-risk areas such as finance, employment and criminal justice. This requires a thorough re-examination of sectorial laws to make sure that they are updated to address the risk of algorithmic decision-making, as most anti-discrimination laws focus on preventing discrimination in human decisions but fall short of addressing the opacity and unpredictability of algorithms.⁶⁰

3. Building up a repertoire of privacy-enhancing technology, and developing a framework of decision-making

A broad range of technology solutions or methods have emerged to achieve specific privacy or data protection functionality, which include encryption, metadata and digital rights management, application programming, system development governance, identity management etc. Besides the well-known methods of deidentification and pseudonymization, synthetic data is another approach to depersonalizing data. Synthetic data is “fake” data that has the same statistical properties as real data, and can be used as a proxy for real data in AI and machine learning, software testing and other purposes.⁶¹ While deidentification, pseudonymization and synthetic data focus on the transformation of data, other technologies approach data protection through the control of data. Recently, a group

of epidemiologists and data scientists in the UK carried out a study of COVID-19-related deaths among various groups of people and, instead of extracting the sensitive medical records of 17 million people from databases, developed software to run the analysis directly on the data.⁶² This approach of sharing and running analysis over sensitive data allows the control of data without moving it or giving it away.⁶³

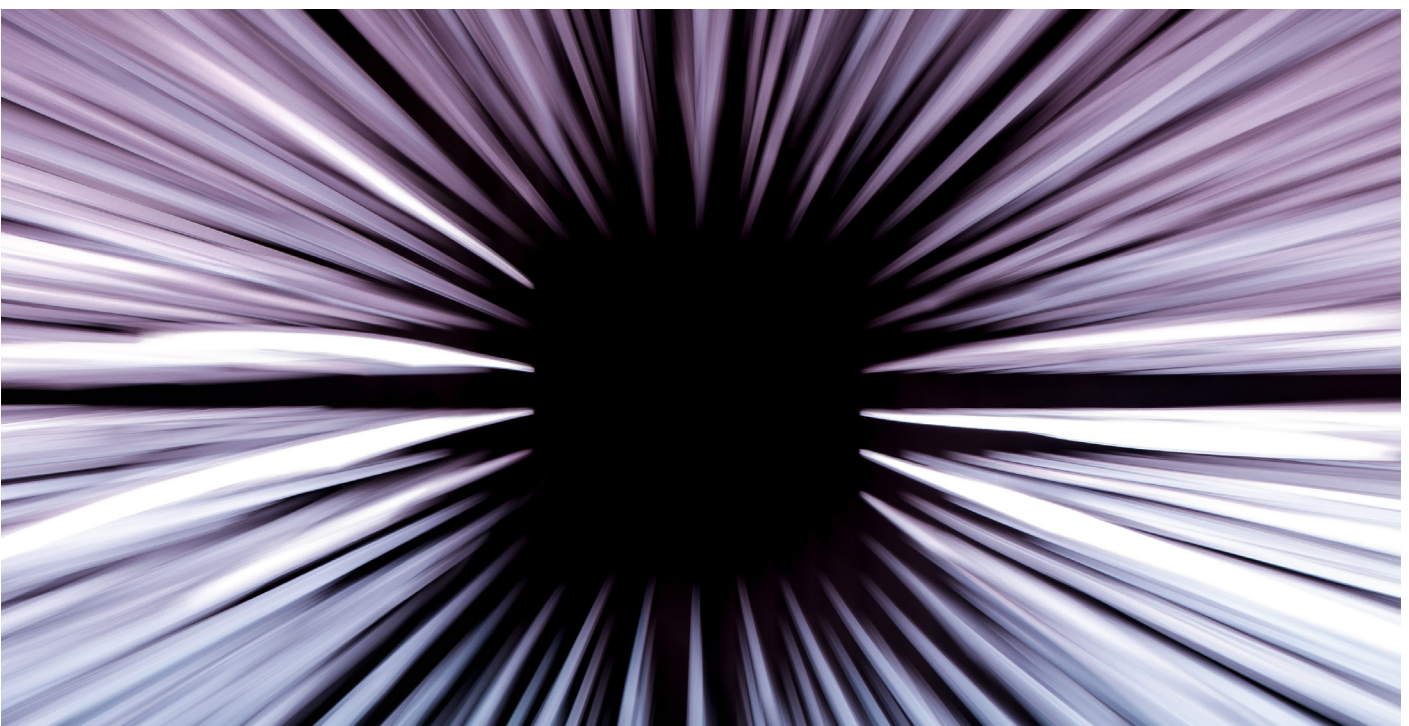
As privacy compliance should be considered as a spectrum of risks, the specific choice of privacy-enhancing technology is often considered along with other factors such as data utility and operational cost. A framework for decision-making can help optimize the solution in each case to protect the privacy of the individual's data.⁶⁴

4. Supporting data subjects and experimenting with the solidarity approach

Responsible use of technology should respect human rights and ethics.⁶⁵ In order to fully realize the social benefits of IoB technology and data, users should be empowered with the legal rights of a data subject and a supporting system to execute those rights. This requires a clearer definition of data ownership and better control of users' own data. Users will be supported with the knowledge of how their data is used, and the ability to access and correct their information, including the means to address unfair inferences and analytics.

In response to social sorting and stratification powered by big-data analysis, some experts

advocate a solidarity approach to health data governance (one focused on societal and community good).⁶⁶ This shifts the focus to the shared societal benefits and responsibilities, which motivates people to share data for the collective and individual good. Biobanks are a good example for sharing biological data. The solidarity approach of data governance treats data contributors as partners, and this involves explicit acknowledgement of the types of research that the database supports, and easy access for community members to research findings. Data subjects should also be informed of the potential risks associated with the participation.⁶⁷



Contributors

Lead Author

Xiao Liu

McGill University Faculty Fellow at the World Economic Forum Centre for the Fourth Industrial Revolution; Wilson China Fellow Steering Committee

Steering Committee

Jeff Merritt

Head, IoT, Robotics and Smart Cities, Centre for the Fourth Industrial Revolution, World Economic Forum

Karime Kuri Tiscareno

Project Lead, IoT, Robotics and Smart Cities, Centre for the Fourth Industrial Revolution, World Economic Forum

Expert Community

This white paper benefitted from the input of many experts and diverse stakeholders who shared case studies, insights and lessons learned through a series of interviews and conversations in 2020.

Ifeoma Ajunwa

Associate Professor of Labor and Employment Law, Cornell University; Faculty Associate, Berkman Klein Center at Harvard Law School

Glenn Cohen

James A. Attwood and Leslie Williams Professor of Law, Harvard Law School; Faculty Director, Petrie-Flom Center for Health Law Policy, Biotechnology & Bioethics

Jim Dempsey

Executive Director, Berkeley Center for Law & Technology

Khaled El Emam

Senior Scientist, CHEO Research Institute; Professor, Pediatrics, Faculty of Medicine, University of Ottawa; Chief Executive Officer, Privacy Analytics

Tad Funahashi

Kaiser Permanente/SCPMG, Chief Innovation Officer, Orthopedic Surgery and Sports Medicine

Jodi Halpern

Professor of Bioethics and Medical Humanities, University of California, Berkeley

Jiang Li

Chief Executive Officer, VivaLNK, Connected Healthcare Solutions

Xuan Hong Lim

Senior Manager, Smart Nation and Digital Government Group, Government of Singapore

Alex Mihailidis

Associate Vice-President – International Partnerships, University of Toronto; Scientific Director – AGE-WELL NCE

Piers Nash

Chief Executive Officer, Sympatic

Kim Old

Chief Commercial Officer, EMOTIV

Olivier Oullier

President, EMOTIV, USA

Margaret Foster Riley

Professor of Law, University of Virginia

Lee Tien

Senior Staff Attorney and Adams Chair for Internet Rights, Electronic Frontier Foundation

Jennifer M. Urban

Clinical Professor of Law Director of Policy Initiatives, Samuelson Law, Technology & Public Policy Clinic, University of California, Berkeley

Sandra Wachter

Associate Professor and Senior Research Fellow, Oxford Internet Institute, University of Oxford

Acknowledgments

This white paper benefitted from insights, comments, conversations and contributions from colleagues at the Centre for the Fourth Industrial Revolution of the World Economic Forum. Special thanks to:

Kimmy Bettinger

Specialist, IoT, Robotics and Smart Cities, World Economic Forum Centre for the Fourth Industrial Revolution

Lynsey Chediak

Project Lead, Precision Medicine, World Economic Forum Centre for the Fourth Industrial Revolution

Anne Josephine Flanagan

Project Lead, Data Policy, World Economic Forum Centre for the Fourth Industrial Revolution

Arthur Hermann

Kaiser Permanente, Alumnus Fellow to the World Economic Forum

Austin Hunter

Specialist, Data Policy, World Economic Forum Centre for the Fourth Industrial Revolution

Eddan Katz

Platform Curator: Artificial Intelligence, World Economic Forum Centre for the Fourth Industrial Revolution; Alumnus Fellow to the World Economic Forum

Elissa Prichep

Project Lead, Precision Medicine, World Economic Forum Centre for the Fourth Industrial Revolution

Geoff Wylde

Project Lead, IoT, Robotics and Smart Cities, World Economic Forum Centre for the Fourth Industrial Revolution

Endnotes

1. Managing Epidemics with Consumer Wearables, World Economic Forum: <https://www.weforum.org/covid-action-platform/projects/managing-epidemics-with-consumer-wearables> (link as of 1/7/20).
2. Andrea M. Matwyshyn, The Internet of Bodies, William & Mary Law Review, Vol. 61, No. 1, 2019.
3. Ibid.
4. Ibid.
5. For example, in the United States, the FDA considers a product to be a device, and subject to FDA regulation, if it meets the definition of a medical device per Section 201(h) of the Food, Drug, and Cosmetic Act. Medical devices are: a) recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them; b) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals; c) or intended to affect the structure or any function of the body of man or other animals. See <https://www.fda.gov/medical-devices/classify-your-medical-device/how-determine-if-your-product-medical-device#steps>.
6. Thousands of Swedes Are Inserting Microchips Under Their Skin, NPR, 2018: <https://www.npr.org/2018/10/22/658808705/thousands-of-swedes-are-inserting-microchips-under-their-skin> (link as of 1/7/20).
7. I Got a Chip Implanted in a Biohacking Garage, Freethink, 2020: <https://www.freethink.com/videos/biohacking> (link as of 1/7/20).
8. Valuates Report, Wearable Technology Market Size is Expected to Reach USD \$57,653 Millions by the End of 2022, With a CAGR of 16.2, PR Newswire, Feb 2020: <https://www.prnewswire.com/news-releases/wearable-technology-market-size-is-expected-to-reach-usd-57-653-millions-by-the-end-of-2022--with-a-cagr-of-16-2--valuates-reports-301001809.html> (link as of 1/7/20).
9. See IDTechEX's market research report, Electronic Skin Patches 2019–2029: <https://www.idtechex.com/en/research-report/electronic-skin-patches-2019-2029/674> (link as of 1/7/20).
10. Ryan Kraudel, National Wearables Survey Reveals Accelerating Convergence of Consumer Wearables and Personal Health & Medical Devices, Valencell, November 2019: <https://valencell.com/press/2018/11/national-wearables-survey-reveals-accelerating-convergence-of-consumer-wearables-and-personal-health-medical-devices/> (link as of 1/7/20).
11. A good example of this: Alex Mihailidis and his team of Intelligent Assistive Technology and Systems Lab in Toronto have been developing a supportive intelligent environment to assist patients and older users with health-monitoring and fall-detecting functions.
12. VivaLNK Offers Rapid Deployment Remote Patient Monitoring Solution with Alibaba, PR Newswire, March 2020: <https://www.prnewswire.com/news-releases/vivalnk-offers-rapid-deployment-remote-patient-monitoring-solution-with-alibaba-301013155.html> (link as of 1/7/20).
13. Agam Shah, Kaiser Permanente Bets on Smartwatches to Lower Costs, Wall Street Journal, January 2020: <https://www.wsj.com/articles/kaiser-permanente-bets-on-smartwatches-to-lower-costs-11578565801> (link as of 1/7/20).
14. Five Years and 500 Fitbit Research Studies, Fitabase, December 2017: <https://www.fitabase.com/blog/post/five-years-500-fitbit-research-studies/> (link as of 1/7/20).
15. IBM Helps Organizations Monitor Their Workers' Safety with Watson IoT, IBM, February 2019: <https://newsroom.ibm.com/2019-02-13-IBM-Helps-Organizations-Monitor-Their-Workers-Safety-with-Watson-IoT> (link as of 1/7/20).
16. Julie Weed, Wearable Tech that Tells Drowsy Truckers It's Time to Pull Over, New York Times, February 2020: <https://www.nytimes.com/2020/02/06/business/drowsy-driving-truckers.html> (link as of 2/7/20).
17. Maarten Falter et. al, Accuracy of Apple Watch Measurements for Heart Rate and Energy Expenditure in Patients with Cardiovascular Disease: Cross-Sectional Study, JMIR Mhealth Uhealth 2019; Vol. 7, No. 3, March 2019, e11889: <http://doi.org/10.2196/11889> (link as of 1/7/20).
18. Emily J. Shiffer, How Accurate Is Apple Watch's Heart Rate Monitor for Detecting Afib? It Can't Replace Medical-Grade Devices, Insider, May 2020: <https://www.insider.com/how-accurate-is-apple-watch-heart-rate> (link as of 1/7/20).
19. Zoë LaRock, Last Year Healthcare Had More Cybersecurity Breaches than Any Other Industry — and It Will Likely Intensify, Business Insider, April 2019: <https://www.businessinsider.com/why-healthcare-data-breach-epidemic-will-intensify-2019-4> (link as of 1/7/20).
20. Alfred Ng, These Kids' Smartwatches Have Security Problems as Simple as 1-2-3, CNet, December 2019: <https://www.cnet.com/news/these-kids-smartwatches-have-security-problems-as-simple-as-1-2-3/> (link as of 1/7/20).
21. Liz Sly, US Soldiers Are Revealing Sensitive and Dangerous Information by Jogging, Washington Post, January 2019: https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html (link as of 1/7/20).
22. Jane C. Hu, So About that Thermometer Data that Says Fevers Are on the Decline, Slate, April 2020: <https://slate.com/technology/2020/04/kinsa-smart-thermometer-data-fevers-covid19.html> (link as of 1/7/20).

23. Florence Hudson and Chris Clark, Wearables and Medical Interoperability: The Evolving Frontier, *Computer*, Vol. 51, No. 9, 2018, pp. 86–90, doi:10.1109/MC.2018.3620987 (link as of 1/7/20).
24. Marshall Allen, Health Insurers Are Vacuuming up Details about You – and It Could Raise Your Rates, *ProPublica*, July 2018: <https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates> (link as of 1/7/20); Mohana Ravindranath, How Your Health Information Is Sold and Turned into Risk Scores, *Politico*, February 2019: <https://www.politico.com/story/2019/02/03/health-risk-scores-opioid-abuse-1139978> (link as of 1/7/20).
25. Ifeoma Ajunwa points out that extant Privacy Protection Acts always contain employer-centric exceptions, and case law has shown that few protections exist when an employee consents to information gathering. See Ifeoma Ajunwa, Algorithms at Work: Productivity Monitoring Platforms and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law, *St. Louis Law Journal*, 21 (2019). There are already multiple lawsuits concerning suspicious employer behaviour in relation to employee wellness plans and work productivity apps. See Ajunwa et al, Limitless Worker Surveillance, *California Law Review*, Vol. 105, No. 3, 2017, pp. 735–776; and Ajunwa, Algorithms at Work.
26. Miranda Bogen, All the Ways Hiring Algorithms Can Introduce Bias, *Harvard Business Review*, 6 May 2019: <https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias> (link as of 6/7/20).
27. See Katherine Kellogg et al., Algorithm at Work: The New Contested Terrain of Control, *Academy of Management*: <https://doi.org/10.5465/annals.2018.0174> (link as of 1/7/20), for more details on how algorithms exacerbate workplace control, and for examples of employees and activists' action to push back against such controls.
28. Lena Solow, The Scourge of Worker Wellness Programs, *New Republic*, September 2019: <https://newrepublic.com/article/154890/scourge-worker-wellness-programs> (link as of 1/7/20).
29. Jessica Bruder, These Workers Have a New Demand: Stop Watching Us, *The Nation*, May 2015: <https://www.thenation.com/article/archive/these-workers-have-new-demand-stop-watching-us/> (link as of 1/7/20); Esther Kaplan, The Spy Who Fired Me, *Harpers*, March 2015: <https://harpers.org/archive/2015/03/the-spy-who-fired-me/2/> (link as of 1/7/20).
30. See Sean McDonald, Ebola: A Big Data Disaster, *CIS Papers*, March 2016: <https://cis-india.org/papers/ebola-a-big-data-disaster> (link as of 1/7/20). Data analytics-based public policy is particularly risky in less-developed countries and among disadvantaged populations where there are no sufficient information and regulatory infrastructures. Linnet Taylor, Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World, in Linnet Taylor et al., editors, *Group Privacy – New Challenges of Data Technologies*, Springer, 2017: pp. 13–36.
31. Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (link as of 1/7/20).
32. Federal Trade Commission Act: <https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act> (link as of 2/7/20).
33. Florent Thouvenin et al., Big Data in the Insurance Industry: Leeway and Limits for Individualising Insurance Contracts: <https://www.jipitec.eu/issues/jipitec-10-2-2019/4916> (link as of 1/7/20).
34. Sharona Hoffman, Big Data's New Discrimination Threats: Amending the Americans with Disabilities Act to Cover Discrimination Based on Data-Driven Predictions of Future Disease, in I. Glenn Cohen et al., editors, *Big Data, Health Law and Bioethics*, Cambridge University Press, 2018, pp. 85–97.
35. For an overview of state privacy laws, see Andy Green, Complete Guide to Privacy Laws in the US, *Varonis*, March 2020: <https://www.varonis.com/blog/us-privacy-laws/> (link as of 1/7/20).
36. Kathryn C. Montgomery, Jeff Chester et al., Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection, Center for Digital Democracy, August 2017: <https://www.democraticmedia.org/CDD-Wearable-Devices-Big-Data-Report> (link as of 1/7/20).
37. Charter of Fundamental Rights of the European Union 2012/C 326/02: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN> (link as of 1/7/20).
38. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications): <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN> (link as of 1/7/20).
39. Art. 4(15) of the GDPR.
40. Art.22 of the GDPR.
41. Sandra Wachter, Affinity Profiling and Discrimination by Association in Online Behavioural Advertising, *Berkeley Technology Law Journal*, Vol. 35, No. 2, 2020.
42. Oliver Jérusalmy and Paul Fox, Insurance and Discrimination – Guaranteeing Full and Equal Access to Insurance, *Finance Watch*, 28 February 2019: <https://www.finance-watch.org/publication/insurance-and-discrimination/> (link as of 1/7/20).
43. W. Nicholson Price II and I. Glenn Cohen, Privacy in the Age of Medical Big Data, *Nature Medicine*, Vol. 25, 2019, pp. 37–43.
44. Kashmir Hill, How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did, *Forbes*, February 2012: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#578f4eeb6668> (link as of 2/7/20).
45. Margaret Foster Riley, Big Data, HIPAA, and the Common Rule: Time for Big Change?, in I. Glenn Cohen et al., editors, *Big Data, Health Law, and Bioethics*, Cambridge University Press, 2018, pp. 251–263.

46. Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, *UCLA Law Review*, Vol. 57, 2010, p. 1701.
47. Mark Rothstein, Is Deidentification Sufficient to Protect Health Privacy in Research? *The American Journal of Bioethics*, Vol. 10, No. 9, September 2010, pp. 3–11, doi: [10.1080/15265161.2010.494215](https://doi.org/10.1080/15265161.2010.494215) (link as of 2/7/20).
48. Sandra Wachter and Brent Mittelstadt, A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI, *Columbia Business Law Review*, 2019 (2).
49. Wachter, Affinity Profiling and Discrimination by Association in Online Behavioural Advertising.
50. Alessandro Mantelero, The Future of Consumer Data Protection in the EU: Re-thinking the “Notice and Consent” Paradigm in the New Era of Predictive Analytics, *Computer Law & Security Review*, Vol. 30, No. 6, 2014, pp. 643–660.
51. Barbara J. Evans, Big Data and Individual Autonomy in a Crowd, in I. Glenn Cohen et al., editors, *Big Data, Health Law, and Bioethics*, Cambridge University Press, 2018, pp. 19–29.
52. Alessandro Mantelero, Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection, *Computer Law and Security Review*, Vol. 32, No. 2, 2016, pp. 238–255.
53. Ibid.
54. Brent Mittelstadt, From Individual to Group Privacy in Big Data Analytics, *Philosophy & Technology*, 30, 2017, 4, pp. 475–494.
55. Matwyshyn, *The Internet of Bodies*.
56. Protecting Personal Health Data Act: <https://www.congress.gov/bill/116th-congress/senate-bill/1842/text/is> (link as of 1/7/20).
57. Linnet Taylor, Luciano Floridi et al., editors, *Group Privacy: New Challenges of Data Technologies*, Springer, 2017; Mantelero, Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection.
58. Ibid.
59. See Wachter and Mittelstadt, A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI; and Wachter, Affinity Profiling and Discrimination by Association in Online Behavioural Advertising.
60. Interview with Sandra Wachter by Xiao Liu on 22 May 2020.
61. See What is Synthetic Data?, *Replica Analytics*: <https://www.replica-analytics.com/synthesis-tutorials> (link as of 2/7/20).
62. The Pandemic Has Spawned a New Way to Study Medical Records, *The Economist*, May 2020: <https://www.economist.com/science-and-technology/2020/05/14/the-pandemic-has-spawned-a-new-way-to-study-medical-records> (link as of 2/7/20).
63. The cloud technology of Sympatic, called “VirtualVault”, is another example of this approach to allow the “computer” to come to the data. See <https://www.sympatic.com> (link as of 1/7/20).
64. Canadian researcher Khaled El Emam developed a framework based on existing research and business practices that takes into consideration different factors, from privacy protection, data utility and operational cost to consumer trust. Data controllers can assign weight to these factors according to regulatory requirements and their own practical needs and find a best combination of solutions. See When to Synthesize: <https://www.replica-analytics.com/synthesis-tutorials> (link as of 1/7/20).
65. For an ethics-based approach to responsible technology, see *Responsible Use of Technology*, World Economic Forum white paper, August 2019: http://www3.weforum.org/docs/WEF_Responsible_Use_of_Technology.pdf (link as of 1/7/20)
66. Barbara Prainsack and Ine Van Hoyweghen, Shifting Solidarities: Personalisation in Insurance and Medicine, in Ine Van Hoyweghen, Valeria Pulignano and Gert Meyers, editors, *Shifting Solidarities: Trends and Developments in European Societies*, Palgrave Macmillan, 2020 (forthcoming). Preview available at: https://www.researchgate.net/publication/338254212_Shifting_Solidarities_Personalisation_in_insurance_and_medicine (link as of 1/7/20).
67. Ibid.



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org